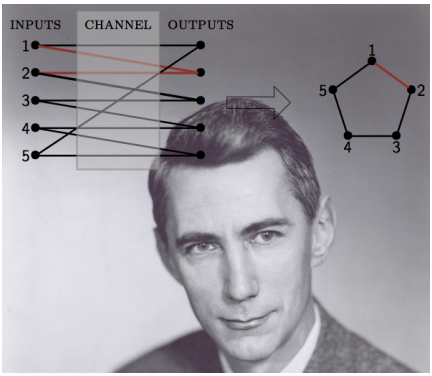
5 Grafentheorie en communicatie
Jop Briët

Voorwoord



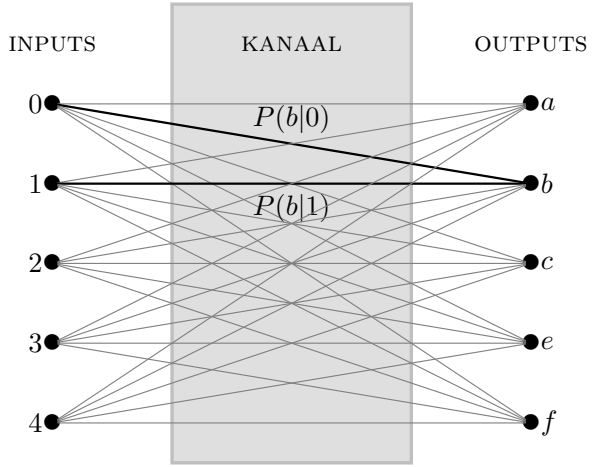
Claude Shannon, vader van de moderne informatietheorie, zette rondom 1950 wiskundige modellen uiteen waarmee communicatie over kanalen met ruis formeel bestudeerd kan worden [Sha48]. Hij liet onder andere zien dat het extreme model waarin berichten altijd perfect moeten aankomen volledig gekarakteriseerd wordt door eigenschappen van simpele grafen [Sha56]. Zo hoort bij ieder kanaal een graaf waarvan de 'Shannon capaciteit' gelijk is aan de maximale communicatiesnelheid die behaald kan worden door middel van codes die berichten moeten beschermen tegen ruis. Het aantal gevolgen dat deze observatie heeft gehad voor de ontwikkeling van de grafentheorie is moeilijk te overschatten.

Een belangrijke tegenhanger van communicatie onder ruis is *broncodering*, waarin twee gescheiden partijen gebruik proberen te maken van bestaande patronen in de informatie waarover ze beschikken om zo efficiënt mogelijkheid informatie uit te wisselen. Analoog aan Shannons observatie merkte Witsenhausen op dat ook dit probleem volledig bestudeerd kan worden aan de hand van eigenschappen van grafen [Wit76].

Het doel van deze tekst is om deze verbanden bloot te leggen en de relevante graafparameters en -concepten te bestuderen. We dekken slechts een minuscuul deel van de reusachtige hoeveelheid literatuur over dit onderwerp ("zero-error information theory") en verwijzen naar Körner en Orlitsky [KO98] voor een uitgebreid overzicht en naar Lubetzky [Lub07] voor meer recente resultaten.

5.1 Kanaalcodering

Een discreet communicatiekanaal met ruis wordt gemodelleerd als een drietal $\mathcal{N} = (S, R, P)$ bestaande uit een eindige verzameling *inputs* S, een eindige verzameling *outputs* R en een kansverdeling $P(\cdot|s)$ over de outputverzameling R voor elke input $s \in S$; zie Figuur 5.1. Het ruismodel dat hiermee vertegenwoordigd wordt dicteert dat als een verzender input $s \in S$ door het kanaal $\mathcal{N}$ stuurt, de ontvanger het signaal $r \in R$ ontvangt met kans $P(r|s)$. We zullen aannemen dat kanalen *geheugenloos* zijn, wat wil zeggen dat als de verzender opeenvolgend inputs s en t (in S) verstuurt, de kans dat de ontvanger respectievelijk signalen q en r (in R) ontvangt gegeven is door het product $P(q|s)P(r|t)$.



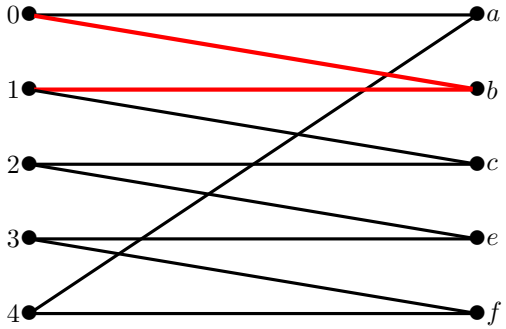
Figuur 5.1: Een discreet kanaal met 5 inputs en 5 outputs. De kans op output b na input 0 of 1 is respectievelijk $P(b|0)$ of $P(b|1)$.

Ruisloos communiceren. Shannon vroeg hoe efficiënt er gecommuniceerd kan worden als de kans op error, misinterpretatie van het verzonden bericht, nul moet zijn. Dit is onmogelijk als de transitiekansen $P(r|s)$ strikt groter zijn dan nul voor elke $s \in S$ en $r \in R$, aangezien de ontvanger dan nooit zeker kan weten wat het oorspronkelijke bericht was. Om te zien wanneer er wel iets te halen valt introduceren we de hoofdrolspeler van deze tekst: de *graaf*.

Definitie 5.1.1 (Graaf)**.** *Een* graaf *is een tweetal* $G = (V, E)$ *bestaande uit een eindige verzameling* V*, waarvan de elementen* knopen *genoemd worden, en een verzameling* E *bestaande uit ongeordende paren* $u, v \in V$*, waarvan de elementen* kanten *genoemd worden. Kanten zullen hier uitsluitend bestaan uit twee verschillende knopen. Voor een kant schrijven we* $\{u, v\} \in E$*.*

Definitie 5.1.2 (Bipartiete graaf)**.** *Een graaf* $G = (V, E)$ *is* bipartiet *als de knopenverzameling* V *bestaat uit een disjuncte vereniging* $V = L \cup R$ *en als* E *uitsluitend kanten van de vorm* $\{u, v\}$ *met* $u \in L$ *en* $v \in R$ *bevat.*

Bekijk nu de versie van Figuur 5.1 waarin input s en output r alleen met elkaar verbonden zijn als $P(r|s) > 0$.

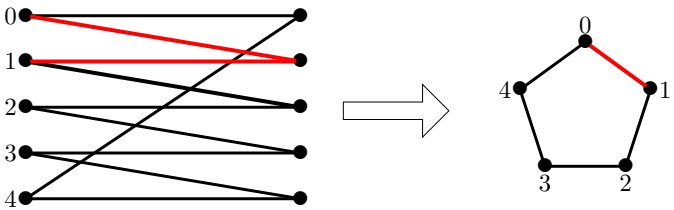


Figuur 5.2: De bipartiete graaf van het kanaal uit Figuur 5.1.

Dit resulteert in een bipartiete graaf zoals bijvoorbeeld die in Figuur 5.2. Als de ontvanger het signaal b ontvangt dan kan die afkomstig zijn geweest van beide inputs 0 en 1. In eerste instantie lijkt het er dus misschien op alsof zelfs in dit geval niet perfect gecommuniceerd kan worden. Dit kan echter wel als de partijen van tevoren afspreken dat slechts een subset van de inputs gebruikt wordt. Bijvoorbeeld, als de verzender alleen inputs 0 en 2 gebruikt, dan zal de ontvanger nooit in verwarring zijn omdat er geen output is die van beide deze inputs afkomstig kan zijn. Dit laat zien dat elke keer dat dit kanaal gebruikt wordt er minstens één bit perfect verstuurd kan worden.

Shannon realiseerde zich dat het aantal berichten dat perfect verstuurd kan worden precies overeenkomt met een bekende graafparameter van de volgende zogeheten *verwarringsgraaf*. De knopen van de verwarrings-

graaf $G = (V, E)$ zijn de inputs van het kanaal, dus $V = S$. Twee knopen $u, v \in V$ vormen een kant als er een $r \in R$ is zodat beide $P(r|v) > 0$ en $P(r|w) > 0$ geldt (zie Figuur 5.3). Met andere woorden, de kanten zijn precies de paren inputs die niet met zekerheid van elkaar onderscheiden kunnen worden.



Figuur 5.3: Van een communicatiekanaal naar zijn verwarringsgraaf.

De relevante graafparameter is het *onafhankelijkheidsgetal* $\alpha(G)$, gedefiniëerd als de grootte van de grootste verzameling knopen die onderling geen kanten vormen, ofwel een onafhankelijke verzameling vormen. Zo komen we op de eerste stelling.

Propositie 5.1.3. *Voor een kanaal met verwarringsgraaf G is $\alpha(G)$ het maximale aantal berichten dat zonder ruis gecommuniceerd kan worden.*

Het voorbeeld uit Figuur 5.3 geeft als verwarringsgraaf de 5-cykel C_5, waarvoor $\alpha(C_5) = 2$ geldt.

Opgave 5.1.4. *Zij $\mathcal{N} = (S, R, P)$ het kanaal met*

$$S = R = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

en waarvoor $P(x|y) = 1/4$ voor alle paren $x \in R, y \in S$ die hetzelfde zijn of in precies één coördinaat verschillen en $P(x|y) = 0$ voor alle andere paren. Wat is de verwarringsgraaf van $\mathcal{N}$ en wat is diens onafhankelijkheidsgetal?

Een algemene vorm van Opgave 5.1.4 vraagt naar het onafhankelijkheidsgetal voor het kanaal waar voor twee natuurlijk getallen d, n zodat $1 \leq d \leq n$, de in- en outputverzamelingen bestaan uit alle reeksen van n bits, dat wil zeggen $S = R = \{0, 1\}^n$, waar $P(x|y) > 0$ voor alle paren x, y die verschillen in hooguit d coördinaten en waar $P(x|y) = 0$ voor alle overgebleven paren. Het antwoord voor $n = 17$ en $d = 6$ is onbekend!

De Shannon capaciteit. In het *kanaalcodering probleem* heeft de verzender een verzameling van m mogelijke berichten die ze zonder ruis naar een ontvanger moet kunnen sturen met behulp van een geheugenloos kanaal $\mathcal{N}$ met verwarringsgraaf $G = (V, E)$. Hierboven zagen we dat als $m \leq \alpha(G)$ geldt, dit probleem opgelost kan worden door elk bericht te coderen als een unieke input van een onafhankelijke verzameling van grootte m in G. Voor elk bericht hoeft het kanaal dan maar één keer gebruikt te worden.

Wat als $m > \alpha(G)$? Een makkelijke oplossing is om de berichten te coderen als reeksen van n inputs uit een onafhankelijke verzameling van grootte $\alpha(G)$, waar de *bloklengte* n gekozen wordt zodat $\alpha(G)^n \geq m$. Elke reeks zal ontvangen worden als een unieke reeks outputs, waardoor de ontvanger de verzender luid en duidelijk kan verstaan. Van het voorbeeld uit Figuur 5.3 zien we bijvoorbeeld dat als $m = 5$, we met bloklengte $n = 3$ toekunnen; er kunnen dan 8 mogelijke berichten verstuurd worden.

Maar dit kan efficiënter! De vraag die we moeten stellen is:

Wanneer kunnen twee inputreeksen $u_1, \ldots, u_n \in S$ en $v_1, \ldots, v_n \in S$ met zekerheid onderscheiden worden?

Als deze reeksen verstuurd worden ontvangt de ontvanger respectievelijk signaalreeksen $x_1, \ldots, x_n \in R$ en $y_1, \ldots, y_n \in R$. Merk op dat als er een $i \in \{1, \ldots, n\}$ is waarvoor u_i en v_i verschillend zijn en géén kant vormen in de verwarringsgraaf, de signalen x_i en y_i dan nooit hetzelfde zijn. Het antwoord op de vraag luidt daarom:

Als er een coördinaat $i \in \{1, \ldots, n\}$ is zodat $u_i \neq v_i$ en $\{u_i, v_i\} \notin E$.

Twee reeksen kunnen dus alleen *verward* worden als voor *elke* coördinaat geldt dat $u_i = v_i$ of $\{u_i, v_i\} \in E$. Dit motiveert de introductie van de verwarringsgraaf $G^{\boxtimes n} = (V^n, E_n)$ voor inputreeksen van lengte n, wiens knopenverzameling bestaat uit het n-voudig cartesisch product van V met zichzelf en wiens kantenverzameling E_n bestaat uit de paren $(u_1, \ldots, u_n)$, $(v_1, \ldots, v_n)$ waarvoor voor elke i geldt dat $u_i = v_i$ of $\{u_i, v_i\} \in E$.

Definitie 5.1.5 (Sterke graafproduct)**.** *Voor twee grafen $G = (V, E)$ en $H = (W, F)$ is het* sterke graafproduct *$G \boxtimes H$ de graaf met het cartesisch product $V \times W$ als knopenverzameling waarin $(v, w), (v', w') \in V \times W$ een kant vormen als $v = v'$ of $\{v, v'\} \in E$ en $w = w'$ of $\{w, w'\} \in F$.*

Opgave 5.1.6. *Zij G de graaf bestaande uit één kant. Teken $G \boxtimes G$. [Hint: De graaf $G \boxtimes G$ is deze zin al afgebeeld.]*

Opgave 5.1.7. *Laat zien dat het sterke graafproduct associatief is: voor alle grafen G, H, J geldt $G \boxtimes (H \boxtimes J) = (G \boxtimes H) \boxtimes J$.*

Opgave 5.1.8. *Laat zien dat* $G^{\boxtimes n} = G \boxtimes G \boxtimes \cdots \boxtimes G$ *(n maal).*

Zo komen we op onze tweede stelling:

Propositie 5.1.9. *Voor een kanaal met verwarringsgraaf* G *is het maximale aantal berichten dat met inputreeksen van lengte* n *zonder ruis verzonden kan worden gelijk aan* $\alpha(G^{\boxtimes n})$.

De voorgaande discussie suggereerde al de volgende eenvoudige stelling over het gedrag van het onafankelijkheidsgetal onder het sterke graafproduct.

Propositie 5.1.10. *Zij* $G = (V, E)$ *en* $H = (W, F)$ *twee grafen. Dan geldt*

$$\alpha(G \boxtimes H) \geq \alpha(G)\alpha(H).$$

Een direct bewijs volgt uit het feit dat het cartesisch product $I \times J$ van een onafhankelijke verzameling $I \subseteq V$ in G en een onafhankelijke verzameling $J \subseteq W$ in H een onafhankelijke verzameling in $G \boxtimes H$ vormt. Door Propositie 5.1.10 herhaaldelijk toe te passen met de conclusie van Opgave 5.1.8 krijgen we ook de volgende voor de hand liggende gevolgtrekking.

Propositie 5.1.11. *Zij* G *een graaf. Dan geldt*

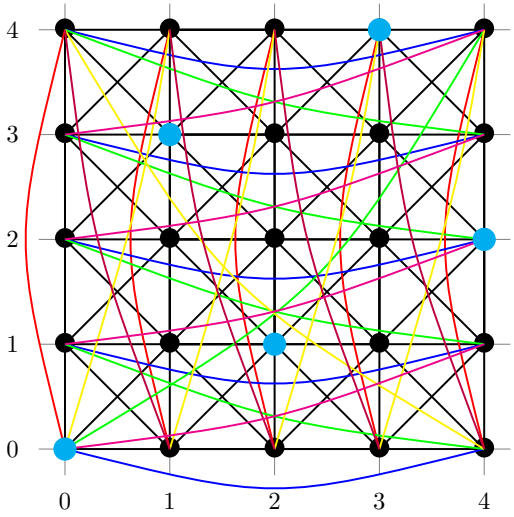
$$\alpha(G^{\boxtimes k}) \geq \alpha(G)^k.$$

De 5-cykel laat al zien dat *blokcoderen*, het coderen van berichten in goed gekozen inputreeksen, kan leiden tot efficiënter gebruik van een kanaal. Shannon merkte op dat de graaf $C_5 \boxtimes C_5$ een onafhankelijke verzameling van grootte 5 heeft: de knopen $(0,0), (2,1), (4,2), (1,3), (3,4)$ vormen onderling geen kanten (zie Figuur 5.4). Over een kanaal met C_5 als verwarringsgraaf kunnen er gemiddeld per input dus geen één, maar minstens $\log_2(5)/2 = 1{,}16\ldots$ bits gecommuniceerd worden.

De Shannon capaciteit van een graaf geeft de maximale communicatiesnelheid wanneer de bloklengte naar oneindig gaat.

Definitie 5.1.12 (Shannon capaciteit)**.** *De* Shannon capaciteit *van een graaf* $G = (V, E)$ *is gedefiniëerd als*

$$\Theta(G) = \lim_{n \to \infty} \alpha(G^{\boxtimes n})^{\frac{1}{n}}.$$



Figuur 5.4: $C_5 \boxtimes C_5$

Wanneer de bloklengte naar oneindig gaat kunnen er gemiddeld per input $\log \Theta(G)$ bits ruisloos verstuurd worden. Helaas is de Shannon capaciteit in het algemeen extreem lastig te bepalen. Zelfs voor de 5-cykel was dit niet eenvoudig. Gegeven dat

$$\sqrt{5} = \alpha(C_5^{\boxtimes 2})^{\frac{1}{2}} > \alpha(C_5) = 2$$

is een natuurlijke vervolgvraag of er wellicht een natuurlijk getal $n \geq 3$ bestaat zodat $\alpha(C_5^{\boxtimes n})^{\frac{1}{n}} > \sqrt{5}$. De vraag naar de exacte waarde van $\Theta(C_5)$ stelde Shannon zelf al in zijn beroemde artikel [Sha56]. Het duurde echter meer dan 20 jaar voordat Lovász [Lov79] met een ingenieus bewijs liet ziet dat Shannons ondergrens van $\sqrt{5}$ niet verbeterd kan worden.

Stelling 5.1.13 (Lovász)**.** *Voor elk natuurlijk getal n geldt*

$$\alpha(C_5^{\boxtimes n})^{1/n} \leq \sqrt{5}.$$

In het bijzonder hebben we $\Theta(C_5) = \sqrt{5}$.

Helaas valt het bewijs van Lovász buiten de strekking van dit artikel, maar dankzij de elegantie ervan is het behalve in de oorspronkelijke bron ook te vinden in het boek *Proofs from THE BOOK* [AZ14, Hoofdstuk 37], vernoemd naar het geheime boek waarin volgens Paul Erdős God de perfecte

bewijzen voor wiskundige stellingen bewaart. Misschien is het verleidelijk te denken dat het bewijs van Lovász de Shannon capaciteit van alle cykels geeft. Zijn algemene resultaat voor oneven cykels luidt als volgt.

Stelling 5.1.14 (Lovász)**.** *Voor $k \geq 3$ oneven geldt*

$$\Theta(C_k) \leq \frac{k \cos\left(\frac{\pi}{k}\right)}{1 + \cos\left(\frac{\pi}{k}\right)}.$$

Voor $k = 5$ geeft dit precies de bovengrens van $\sqrt{5}$. De capaciteit van de 7-cykel is echter nog steeds niet bekend! Stelling 5.1.14 en een recente berekening van [MÖ15] die de, voor de auteur, best-bekende ondergrens geeft, laten zien dat

$$3{,}2271 < 350^{\frac{1}{5}} \leq \alpha(C_7^{\boxtimes 5})^{\frac{1}{5}} \leq \Theta(C_7) < 3{,}3177.$$

De capaciteiten van k-cykels met oneven $k \geq 9$ zijn evenmin bekend. *Even* cykels zijn een ander verhaal. De reden daarvoor is dan deze grafen bipartiet zijn. Voor bipartiete grafen is de Shannon capaciteit *wel* simpel te bepalen.

Propositie 5.1.15. *Zij G een bipartite graaf. Dan geldt*

$$\Theta(G) = \alpha(G).$$

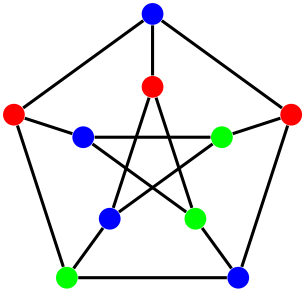
Een grotere klasse grafen waarvoor deze stelling geldt wordt gevormd door de *perfecte grafen*, waar de rest van deze sectie aan gewijd zal worden. De definitie van deze klasse is gebaseerd op de volgende drie basisconcepten.

Definitie 5.1.16 (Clique)**.** *Een* clique *is een deelverzameling knopen waarvan elke twee een kant vormen. Het* cliquegetal *van een graaf G, genoteerd als $\omega(G)$, is het aantal knopen in een clique van maximale grootte.*

Definitie 5.1.17 (Geldige knopenkleuring)**.** *Een* geldige knopenkleuring *van een graaf is een toewijzing van een kleur aan elke knoop zodanig dat elke kant tweekleurig is. Het* chromatisch getal *van een graaf G, genoteerd als $\chi(G)$, is het minimum aantal kleuren voor een geldige knopenkleuring.*

Merk op dat het chromatisch getal altijd minstens het cliquegetal is.

Definitie 5.1.18 (Geïnduceerde deelgraaf)**.** *Zij $G = (V, E)$ een graaf en $S \subseteq V$ een deelverzameling. De* deelgraaf geïnduceerd door S *is de graaf met knopenverzameling S en wiens kantenverzameling bestaat uit de kanten in $\{u, v\} \in E$ zodanig dat $u, v \in S$.*



Figuur 5.5: De Petersen graaf heeft cliquegetal 2 en chromatisch getal 3.

De Petersen graaf in Figuur 5.5 heeft bijvoorbeeld het pentagon als geïnduceerde deelgraaf. De definitie van een perfecte graaf is nu als volgt.

Definitie 5.1.19 (Perfecte graaf)**.** *Een graaf is* perfect *als voor elke geïnduceerde deelgraaf geldt dat het chromatisch getal gelijk is aan het cliquegetal.*

De Petersen graaf (Figuur 5.5) is een voorbeeld van een graaf die *niet* perfect is, omdat het cliquegetal van de graaf zelf verschilt van zijn kleurgetal. Het is niet moeilijk te zien dat bipartite grafen perfect zijn omdat ze chromatisch getal 2 hebben. Zoals hierboven al aangekondigd hebben we de volgende stelling over de Shannon capaciteit van perfecte grafen.

Stelling 5.1.20. *Zij G een perfecte graaf, dan geldt*

$$\Theta(G) = \alpha(G).$$

In het resterende deel van deze sectie zullen wij deze stelling bewijzen. Hiervoor introduceren we twee laatste graafconcepten.

Definitie 5.1.21 (Graaf complement)**.** *Het* complement *van een graaf $G = (V, E)$, aangeduid als $\overline{G}$, heeft V als knopenverzameling en twee knopen vormen een kant dan en slechts dan als ze* geen *kant in G vormen.*

Definitie 5.1.22 (Disjunctieve graafproduct)**.** *Voor grafen $G = (V, E)$ en $H = (W, F)$ is het* disjunctieve graafproduct *$G \vee H$ de graaf met knopenverzameling $V \times W$ waarin $(v, w), (v', w') \in V \times W$ een kant vormen als $\{v, v'\} \in E$ of $\{w, w'\} \in F$.*

Het disjunctieve graafproduct is ook associatief. We kunnen daarom machten nemen: $G^{\vee k} = G \vee G \vee \cdots \vee G$ (k keer).

Het bewijs van Stelling 5.1.20 breken we op in een paar eenvoudige stukken. Eerst relateren we het onafhankelijkheidsgetal van een perfecte graaf aan het chromatisch getal van zijn complement.

Hiervoor gebruiken we de perfecte graaf stelling van Lovász (zie bijvoorbeeld [D05, Stelling 5.5.4]).

Stelling 5.1.23 (Lovász)**.** *Zij G een perfecte graaf. Dan is $\overline{G}$ ook perfect.*

Propositie 5.1.24. *Zij G een perfecte graaf. Dan geldt*

$$\alpha(G) = \chi(\overline{G}).$$

Voor het bewijs van deze propositie, merk op dat $\alpha(G) = \omega(\overline{G})$ en dat een perfecte graaf voldoet aan de eigenschap $\omega(G) = \chi(G)$.

Vervolgens beschouwen we het chromatisch getal van disjunctieve graafproducten en krijgen we een tegenhanger van Stelling 5.1.11.

Lemma 5.1.25. *Voor elke graaf G geldt*

$$\chi(G^{\vee k}) \leq \chi(G)^k.$$

Voor het bewijs nemen we een geldige kleuring van G met $c = \chi(G)$ kleuren. Associeer de kleuren met de getallen $1, \ldots, c$. We "kleuren" vervolgens de graaf $G^{\vee k}$ met reeksen $(c_1, \ldots, c_k) \in \{1, \ldots, c\}^k$ als volgt. We kleuren de knoop $(u_1, \ldots, u_k) \in V^k$ van $G^{\vee k}$ met de reeks $(c_1, \ldots, c_t)$ zodat in de kleuring van G knoop u_i kleur c_i heeft voor elke $i \in \{1, \ldots, k\}$. Knopen $(u_1, \ldots, u_k), (v_1, \ldots, v_k) \in V^k$ vormen een kant in $G^{\vee k}$ als er een $i \in \{1, \ldots, k\}$ is zodat $\{u_i, v_i\} \in E$. Maar in dat geval verschillen de kleuren van die knopen op coödinaat i en hebben we $G^{\vee k}$ dus geldig gekleurd. We hebben hooguit $c^k = \chi(G)^k$ kleuren gebruikt en daarmee is het lemma bewezen.

Het laatste ingrediënt voor het bewijs van Stelling 5.1.20 relateert het sterke graafproduct en het disjunctieve graafproduct.

Lemma 5.1.26. *Voor elke graaf G geldt*

$$\overline{G^{\boxtimes k}} = (\overline{G})^{\vee k}.$$

Voor het bewijs volgen we de definities. Twee knopen $u, v \in V^k$ vormen een kant in $\overline{G^{\boxtimes k}}$ dan en slechts dan als ze *geen* kant vormen in $G^{\boxtimes k}$. Maar

u en v vormen geen kant in $G^{\boxtimes k}$ dan en slechts dan als er een $i \in \{1, \ldots, k\}$ is zodat u_i en v_i verschillen en geen kant in G vormen. De knopen u en v vormen dus een kant in $\overline{G^{\boxtimes k}}$ dan en slecht dan als er een $i \in \{1, \ldots, k\}$ is zodat u_i en v_i een kant vormen in $\overline{G}$. We concluderen dat de kanten van $\overline{G^{\boxtimes k}}$ overeenkomen met de kanten van $(\overline{G})^{\vee k}$ en daarmee is het lemma bewezen.

Met de bovenstaande drie ingrediënten is het bewijs van Stelling 5.1.20 nu eenvoudig. Op een rijtje impliceren ze direct dat voor elke perfecte graaf G en natuurlijk getal k geldt dat

$$\alpha(G^{\boxtimes k}) \leq \chi(\overline{G^{\boxtimes k}}) = \chi((\overline{G})^{\vee k}) \leq \chi(\overline{G})^k = \alpha(G)^k.$$

We concluderen dat

$$\Theta(G) = \lim_{k \to \infty} \alpha(G^{\boxtimes k})^{1/k} = \lim_{k \to \infty} \left(\alpha(G)^k\right)^{1/k} = \alpha(G)$$

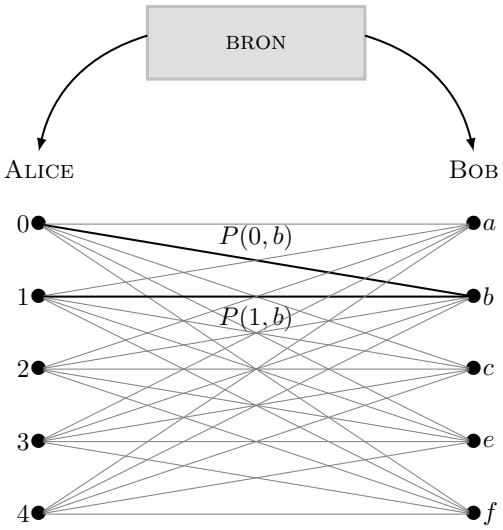
en daarmee is de stelling bewezen.

5.2 Broncodering

In het broncodering probleem krijgen twee partijen, Alice en Bob, allebei een input van een externe bron en is hun doel om met zo min mogelijk communicatie Alices input aan Bob duidelijk te maken. Alice kan hiervoor uiteraard haar hele input naar Bob sturen, maar soms kan er communicatie bespaard worden als Bobs input al wat informatie over die van Alice bevat.

Vergelijkbaar met een discreet kanaal is een *discrete bron* een drietal $\mathcal{M} = (U, W, P)$ bestaande uit een eindige inputverzameling U voor Alice, een eindige inputverzameling W voor Bob en een kansverdeling P over alle mogelijke paren in $U \times W$. Het model dicteert dat de kans dat Alice input $u \in U$ en Bob input $w \in W$ krijgt gegeven is door $P(u, w)$. Zoals voor kanalen met ruis wordt aangenomen dat de bron geheugenloos is, wat wil zeggen dat de kansverdeling P na elke instantie onveranderd blijft.

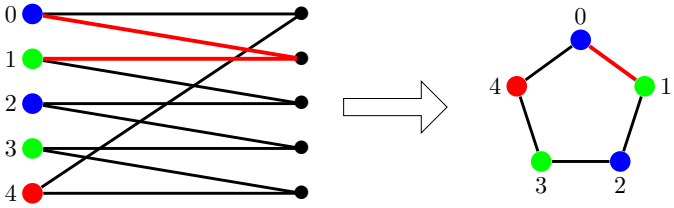
Zoals Shannon voor het kanaalcodering probleem, beschouwde Witsenhausen [Wit76] de minimale communicatie die nodig is in het geval waarin er geen fouten getolereerd kunnen worden, oftewel de maximale snelheid waarmee het probleem opgelost kan worden in het foutloze model. Als voorheen doen de waarden van de kansen $P(u, v)$ er dan niet meer toe en is het alleen van belang of ze nul zijn of niet. Voor de bron van Figuur 5.6 krijgen we zo bijvoorbeeld een graaf die er zo uitziet als die van Figuur 5.2.



Figuur 5.6: Een discrete bron met 5 mogelijke inputs voor Alice en Bob.

Het probleem van foutloze broncodering kan wederom bestudeerd worden in graaftheoretische termen. Hiervoor associëren we met een bron $\mathcal{M} = (U, W, P)$ een zogeheten *karakteristieke graaf* $G = (V, E)$ met knopenverzameling $V = U$ en waarin twee knopen $u, v \in V$ een kant vormen als er een $w \in W$ is zodat beide $P(u, w) > 0$ en $P(v, w) > 0$ gelden (zie Figuur 5.7). De gedachte achter deze graaf is dat als Bob $w \in W$ ontvangt, hij niet weet of Alices input u of v is en Alice hem dus van extra informatie moet voorzien. Met andere woorden, de kanten in de karakteristieke graaf G identificeren precies Alices inputparen die Bob niet altijd kan onderscheiden.

Het oplossen van een broncodering probleem betekend dat Alice voor elk van haar mogelijke inputs een zo kort mogelijk bericht voor Bob heeft waaruit hij haar input kan herleiden. Als we deze berichten zien als kleuren dan moet de kleuring van Alices inputverzameling er aan voldoen dat paren van inputs die door Bob mogelijk verward kunnen worden verschillende kleuren hebben. Met andere woorden, de kleuring moet een geldige kleuring van de karakteristieke graaf zijn! Andersom zien we ook dat een geldige kleuring van de karakteristieke graaf gebruikt kan worden om het broncodering probleem op te lossen. De eerste stelling voor het broncode-



Figuur 5.7: Van een bron naar z'n karakteristieke graaf.

ring probleem luidt dus:

Stelling 5.2.1. *Het oplossen van één instantie van het broncodering probleem voor een bron met karakteristieke graaf G is equivalent met het vinden van een geldige kleuring van G.*

Als gevolgtrekking zien we ook direct het volgende feit.

Propositie 5.2.2. *Het minimale aantal bits dat Alice Bob kan sturen bij het coderen voor een bron met karakteristieke graaf G is $\lceil \log_2 \chi(G) \rceil$.*

De Witsenhausen snelheid. Broncodering kan soms efficiënter gedaan worden door blokken inputreeksen samen te coderen. Hierbij wachten Alice en Bob totdat ze n paren inputs hebben ontvangen, waarna Alice haar reeks codeert in een zo kort mogelijk bericht waaruit Bob, samen met zijn inputreeks, Alices reeks kan achterhalen. Natuurlijk kan Alices bericht bestaan uit de reeks van n kleuren die ze haar inputs in de individuele instanties zou geven, zodat Bob elk van haar inputs onafhankelijk van elkaar kan achterhalen. In graaftheoretische termen zegt dit dat blokken van n inputs gecodeerd kunnen worden met $\chi(G)^n$ verschillende berichten. Maar, zoals al aangekondigd, kan dit soms efficiënter. De vraag die we moeten stellen is wanneer Bob twee inputreeksen $u_1, \ldots, u_n \in V$ en $v_1 \ldots, v_n \in V$ van Alice niet met zekerheid kan onderscheiden. Merk op dat dit gebeurd wanneer voor *elke* $i \in \{1, \ldots, n\}$ geldt dat $u_i = v_i$ of $\{u_i, v_i\} \in E$, omdat als er één coördinaat i is waarvoor geen van beide dingen gelden, Bob u_i en v_i, en daarom de hele reeksen, kan onderscheiden aan de hand van zijn i'de input. De mogelijk te verwarren paren zijn dus weer precies de kanten van de graaf $G^{\boxtimes n}$! Zo komen we bij de tweede stelling,

Stelling 5.2.3. *Het minimum aantal verschillende kleuren (codewoorden) dat Alice kan gebruiken is $\chi(G^{\boxtimes n})$.*

De volgende definitie volgt daarom als een natuurlijke tegenhanger van de Shannon capaciteit.

Definitie 5.2.4 (Witsenhausen snelheid)**.** *De* Witsenhausen snelheid *van een graaf G is gedefiniëerd als*

$$R(G) = \lim_{n\to\infty} \chi(G^{\boxtimes n})^{\frac{1}{n}}.$$

Als de bloklengte naar oneindig gaat hoeven er gemiddeld $\lceil \log_2 R(G) \rceil$ bits per broninstantie gecommuniceerd te worden.

Hierboven gaven we al een intuïtief bewijs voor de volgende stelling over het gedrag van het chromatisch getal onder het sterke graafproduct.

Propositie 5.2.5. *Zij G een graaf. Dan geldt*

$$\chi(G^{\boxtimes n}) \leq \chi(G)^n.$$

Dat het coderen van blokken een verschil kan maken, met andere woorden, dat $\chi(G^{\boxtimes n}) < \chi(G)^n$ soms kan gelden, is weer te zien aan de hand van ons lopende voorbeeld, de 5-cykel. We weten al dat $\chi(C_5) = 3$. Witsenhausen liet zien dat strikt minder dan 9 kleuren voldoende zijn voor $C_5^{\boxtimes 2}$.

Propositie 5.2.6 (Witsenhausen)**.** $\chi(C_5^{\boxtimes 2}) \leq 5$.

$(0,0)$	$(2,1)$	$(4,2)$	$(1,3)$	$(3,4)$
$(0,1)$	$(2,2)$	$(4,3)$	$(1,4)$	$(3,0)$
$(0,2)$	$(2,3)$	$(4,4)$	$(1,0)$	$(3,1)$
$(0,3)$	$(2,4)$	$(4,0)$	$(1,1)$	$(3,2)$
$(0,4)$	$(2,0)$	$(4,1)$	$(1,2)$	$(3,3)$

Figuur 5.8: Witsenhausens kleuring van $C_5 \boxtimes C_5$.

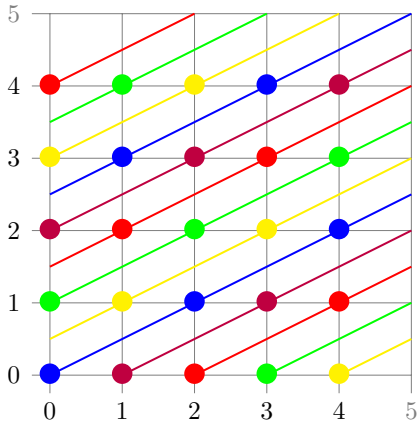
De meest expliciete manier om dit zien is door te verifiëren dat Witsenhausens kleuring (Figuur 5.8) geldig is. Merk allereerst op dat de tabel alle knopen van $C_5 \boxtimes C_5$ bevat. Merk ten tweede op dat elke rij een onafhankelijke verzameling vormt. Omdat elke onafhankelijke verzameling een eigen kleur heeft is de kleuring geldig.

Deze kleuring vond Witsenhausen niet door met veel geduld alle mogelijkheden te doorzoeken. Een vertaling van zijn elegante argument is gebaseerd op tellen modulo 5. Merk op dat twee knopen $x, y \in \{0,1,2,3,4\}$ van

de graaf C_5 een kant vormen als $x - y = 1 \pmod 5$ of $x - y = 4 \pmod 5$. Twee knopen $(x, y), (x', y') \in \{0, 1, 2, 3, 4\} \times \{0, 1, 2, 3, 4\}$ van de graaf $C_5 \boxtimes C_5$ vormen daarom een kant als $(x, y) - (x', y') \pmod 5$ behoort tot de verzameling

$$(0, 1) \quad (1, 0) \quad (1, 1) \quad (0, 4) \quad (4, 0) \quad (1, 4) \quad (4, 1) \quad (4, 4).$$

Beeld de knopen van $C_5^{\boxtimes 2}$ af op een tweedimensionaal grid (Figuur 5.9).

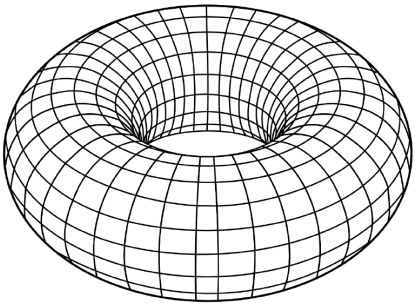


Figuur 5.9: Lijnkleuring van $C_5 \boxtimes C_5$.

Witsenhausen observeerde dat alle knopen op een lijn wiens richting niet gegeven is door één van de punten uit de rij hierboven een onafhankelijke verzameling vormen. De reden hiervoor is dat het verschil van elke twee punten op een lijn in richting (a, b) gelijk is aan een veelvoud van (a, b). Beschouw bijvoorbeeld de lijn door de oorsprong $(0, 0)$ in richting $(2, 1)$ (de blauwe lijn in Figuur 5.9). Modulo 5 bevat deze lijn de punten $(0, 0)$, $(2, 1)$, $2(2, 1) = (4, 2)$, $3(2, 1) = (6, 3) = (1, 3) \pmod 5$ en $4(2, 1) = (8, 4) = (3, 4) \pmod 5$, precies de eerste rij uit Figuur 5.8. Als twee knopen geen kant vormen dan mogen we ze dezelfde kleur geven en omdat we alle knopen kunnen dekken met vijf parallelle lijnen zijn vijf kleuren dus voldoende.

Analoog aan de kanaalsetting gelden de volgende twee stellingen voor de Witsenhausensnelheid van C_5.

Propositie 5.2.7 (Lovász)**.** $R(C_5) = \sqrt{5}$.



Figuur 5.10: Figuur 5.9 had beter op een torus getekend kunnen worden omdat de tegenoverliggende randen aan elkaar gelijmd zijn.

Dit volgt direct uit Stelling 5.1.13, die zei dat $\alpha(C_5^{\boxtimes n}) \leq 5^{n/2}$, en door de volgende eenvoudige observatie toe te passen op de graaf $G = C_5^{\boxtimes n}$:

Propositie 5.2.8. *Zij $G = (V, E)$ een graaf. Dan geldt*

$$\alpha(G)\chi(G) \geq |V|.$$

Waarom is dit zo? Stel we hebben en geldige kleuring van een graaf G met $c = \chi(G)$ knopen. Noem de kleuren $1, 2, \ldots, c$. Voor kleur i, laat n_i het aantal knopen met kleur i zijn. Elke knoop heeft een kleur, dus het totale aantal knopen is $n_1 + n_2 + \cdots + n_c = |V|$. Knopen met eenzelfde kleur moeten een onafhankelijke verzameling vormen. Daarom kan elke kleurklasse uit hooguit $\alpha(G)$ knopen bestaan. We hebben dus dat $n_i \leq \alpha(G)$ voor elke kleur i waaruit de claim volgt.

We sluiten af met een opgave die de bovenstaande twee onderwerpen met elkaar verbindt. Voor meer over dit verband, zie [NTR06].

Opgave 5.2.9 (Kanaal-broncoderen)**.** *Alice en Bob hebben een kanaal met verwarringsgraaf $G = (V, E)$ en een bron met karakteristieke graaf $H = (W, F)$. Om het broncodering probleem op te lossen mogen Alice en Bob alleen gebruik maken van hun kanaal. Waar moeten G en H aan voldoen wil dit kunnen? [Hint: Een* homomorphisme *van een graaf $G' = (V', E')$ naar een graaf $H' = (W', F')$ is een afbeelding van V' op W' zodat elke kant in G' afgebeeld wordt op een kant in H'.]*

Bibliografie

[AZ14] M. Aigner and G.M. Ziegler. *Proofs from The Book*. Springer-Verlag, Berlin, fifth edition, 2014. ISBN 978-3-662-44204-3; 978-3-662-44205-0. Including illustrations by Karl H. Hofmann.

[D05] R. Diestel. *Graph theory*. Graduate Texts in Mathematics, Vol. 173. Springer-Verlag, Berlin, third edition, 2005.

[KO98] J. Körner and A. Orlitsky. Zero-error information theory. *IEEE Trans. Inform. Theory*, 44(6):2207–2229, 1998. Information theory: 1948–1998.

[Lov79] L. Lovász. On the Shannon capacity of a graph. *IEEE Trans. Inform. Theory*, 25(1):1–7, 1979.

[Lub07] E. Lubetzky. *Graph Powers and Related Extremal Problems*. Ph.D. thesis, Tel Aviv University, 2007.

[MÖ15] K.A. Mathew and P.R.J. Östergøard. New lower bounds for the Shannon capacity of odd cycles. *Designs, Codes and Cryptography*, pages 1–10, 2015.

[NTR06] J. Nayak, E. Tuncel, and K. Rose. Zero-error source-channel coding with side information. *Information Theory, IEEE Transactions on*, 52(10):4626–4629, 2006.

[Sha48] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[Sha56] C.E. Shannon. The zero error capacity of a noisy channel. *Institute of Radio Engineers, Transactions on Information Theory*, IT-2(September):8–19, 1956.

[Wit76] H.S. Witsenhausen. The zero-error side information problem and chromatic numbers. *IEEE Trans. Information Theory*, IT-22(5):592–593, 1976.