

Jop Briët

Centrum Wiskunde & Informatica  
Amsterdam  
jop.briet@cwi.nl

## Vakantiecursus

# Grafentheorie en communicatie

Op de vakantiecursus 2016 van het Platform Wiskunde Nederland hield Jop Briët een voordracht over het optimaliseren van communicatie over netwerken met ruis. Door geschikt te coderen kan een foutloze communicatie worden gerealiseerd met maximale snelheid, een en ander afhankelijk van de vorm van het netwerk.

Claude Shannon, vader van de moderne informatietheorie, zette rondom 1950 wiskundige modellen uiteen waarmee communicatie over kanalen met ruis formeel bestudeerd kan worden [8]. Hij liet onder andere zien dat het extreme model waarin berichten altijd perfect moeten aankomen volledig gekarakteriseerd wordt door eigenschappen van simpele grafen [9]. 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 *bruncodering*, waarin gescheiden partijen gebruik maken van bestaande patronen in de informatie waarover ze beschikken om efficiënt informatie uit te wisselen. Analoog aan Shannons observatie merkte Witsenhausen op dat ook dit probleem volledig bestudeerd kan wor-

den aan de hand van eigenschappen van grafen [10]. Het doel van deze tekst is om deze verbanden bloot te leggen en de relevante graafparameters en -concepten te bestuderen. We dekken slechts een minuscule deel van de reusachtige hoeveelheid literatuur over dit onderwerp (‘zero-error information theory’) en verwijzen naar Körner en Orłitsky [3] voor een uitgebreid overzicht en naar Lubetzky [5] voor meer recente resultaten.

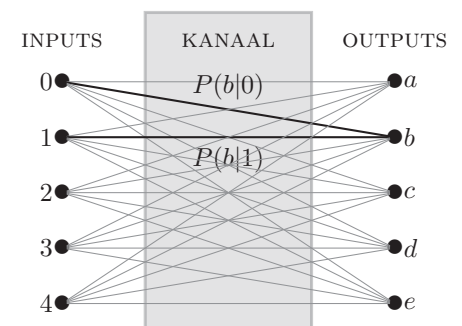
### Kanaalcodering

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 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,

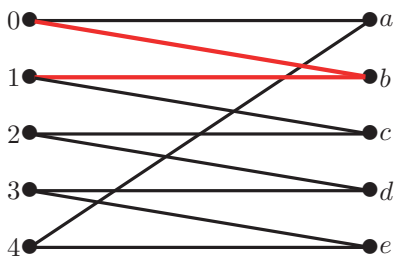
wat wil zeggen dat als de verzender opeenvolgend inputs  $s$  en  $t$  (in  $S$ ) verstuurt, de kans dat de ontvanger respectievelijk signalen  $q$  en  $r$  (in  $R$ ) ontvangt gegeven is door het product  $P(q | s)P(r | t)$ .

### 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 alle transitiekansen  $P(r | s)$  strikt groter zijn dan nul, aangezien de ontvanger dan nooit zeker kan weten wat het oorspronkelijke bericht was. Om te zien wanneer er wel iets te halen valt bekijken we nu de versie van



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



**Figuur 2** De bipartiete graaf van het kanaal uit Figuur 1.

Figuur 1 waarin input  $s$  en output  $r$  alleen met elkaar verbonden zijn als  $P(r|s) > 0$ .

Dit resulteert in een bipartiete graaf zoals bijvoorbeeld die in Figuur 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 verwarringsgraaf  $G = (V, E)$  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  $P(r|u) > 0$  geldt (zie Figuur 3). Met andere woorden, de kanten zijn precies de paren inputs die niet met zekerheid van elkaar onderscheiden kunnen worden.

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

**Propositie 1.** Voor een kanaal met verwarringsgraaf  $G$  is  $\alpha(G)$  het maximale aantal berichten dat zonder ruis gecommuniceerd kan worden.

*De Shannon-capaciteit*

In het *kanaalcoderingsprobleem* 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  $N$  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.

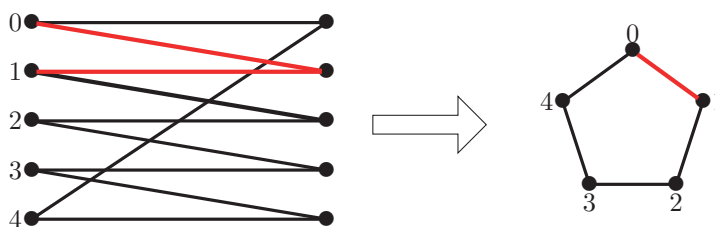
Wat als  $m > \alpha(G)$ ? Een makkelijke oplossing is om de berichten te coderen als reeksen van  $n$  inputs uit een onafhankelijke verzameling van grootte  $\alpha(G)$ , waar de *bloklengte*  $n$  gekozen wordt zodat  $\alpha(G)^n \geq m$ . Elke reeks zal ontvangen worden als een unieke reeks outputs,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

*“Wanneer kunnen twee inputreeksen  $u_1, \dots, u_n \in S$  en  $v_1, \dots, v_n \in S$  met zekerheid onderscheiden worden?”*

Als deze reeksen verstuurd worden ontvangt de ontvanger respectievelijk signaalreeksen  $x_1, \dots, x_n \in R$  en  $y_1, \dots, y_n \in R$ . Merk op dat als er een  $i \in \{1, \dots, n\}$  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  $i \in \{1, \dots, n\}$  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 verwarringsgraaf  $G^{\boxtimes n} = (V^n, E_n)$  voor inputreeksen van lengte  $n$ , waarvan de knopenverzameling bestaat uit het  $n$ -voudig cartesisch product van  $V$  met zichzelf en de kantenverzameling  $E_n$  bestaat uit de paren  $(u_1, \dots, u_n), (v_1, \dots, v_n)$  waarvoor voor elke  $i$  geldt dat  $u_i = v_i$  of  $\{u_i, v_i\} \in E$ .



**Figuur 3** Van een communicatiekanaal naar zijn verwarringsgraaf.

De notatie  $G^{\boxtimes n}$  komt voort uit het feit dat het sterke graafproduct  $G \boxtimes H$  van twee grafen  $G$  en  $H$  associatief is en dat  $G^{\boxtimes n} = G \boxtimes G \boxtimes \dots \boxtimes G$  ( $n$  maal). De graaf  $G \boxtimes H$  heeft  $V \times W$  als knopenverzameling en twee knopen  $(v, w), (v', w') \in V \times W$  vormen een kant als  $v = v'$  of  $\{v, v'\} \in E$  en  $w = w'$  of  $\{w, w'\} \in F$ . Zo komen we op onze tweede stelling:

**Propositie 2.** 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 onafhankelijkheidsgetal onder het sterke graafproduct.

**Propositie 3.** Zij  $G = (V, E)$  en  $H = (W, F)$  twee grafen. Dan geldt

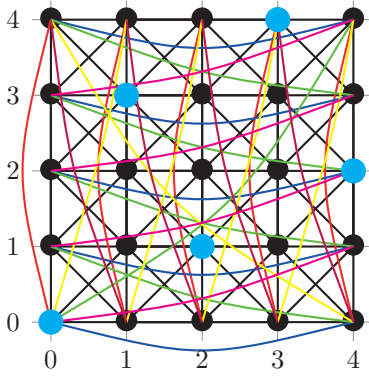
$$\alpha(G \boxtimes H) \geq \alpha(G)\alpha(H).$$

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 3 herhaaldelijk toe te passen krijgen we ook de volgende voor de hand liggende gevolgtrekking.

**Propositie 4.** 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 4). Over een kanaal met  $C_5$  als verwarringsgraaf



Figuur 4  $C_5 \boxtimes C_5$ .

kunnen er gemiddeld per input dus geen één, maar minstens  $\log_2(5)/2 = 1,16\dots$  bits gecommuniceerd worden.

De Shannon-capaciteit van een graaf geeft de maximale communicatiesnelheid wanneer de blok lengte naar oneindig gaat.

**Definitie 1** (Shannon-capaciteit). De *Shannon-capaciteit* van een graaf  $G = (V, E)$  is gedefinieerd als

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

Wanneer de blok lengte 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

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

is een natuurlijke vervolgvraag of er wellicht een natuurlijk getal  $n \geq 3$  bestaat zodat  $\alpha(C_5^{\boxtimes n})^{1/n} > \sqrt{5}$ . De vraag naar de exacte waarde van  $\Theta(C_5)$  stelde Shannon zelf al in zijn beroemde artikel [9]. Het duurde echter meer dan twintig jaar voordat Lovász [4] met een ingenieus bewijs liet zien dat Shannons ondergrens van  $\sqrt{5}$  niet verbeterd kan worden.

**Stelling 1** (Lovász). *Voor elk natuurlijk getal  $n$  geldt*

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

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

Voor het bewijs verwijzen we naar *Proofs from THE BOOK* [1, Hoofdstuk 37], vernoemd naar het geheime boek waarin, volgens Paul Erdős, God de perfecte bewijzen voor wiskundige stellingen bewaart.

De capaciteiten van  $k$ -cyclen met oneven  $k \geq 9$  zijn evenmin bekend. *Even* cyclen zijn een ander verhaal. De reden daarvoor is dat deze grafen bipartiet zijn en daarom behoren tot de klasse *perfecte grafen*. De definitie van deze klasse is gebaseerd op de volgende basisconcepten.

**Definitie 2** (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 3** (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 4** (Geïnduceerde deelgraaf). Zij  $G = (V, E)$  een graaf en  $S \subseteq V$  een deelverzameling. De *deelgraaf geïnduceerd door  $S$*  is de graaf met knopenverzameling  $S$  wiens kantenverzameling bestaat uit de kanten in  $\{u, v\} \in E$  zodanig dat  $u, v \in S$ .

De Petersen-graaf in Figuur 5 heeft bijvoorbeeld het pentagon als geïnduceerde deelgraaf. De definitie van een perfecte graaf is nu als volgt.

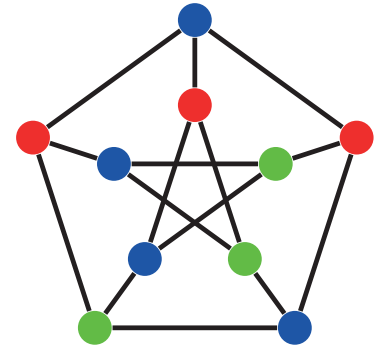
**Definitie 5** (Perfecte graaf). Een graaf is *perfect* als voor elke geïnduceerde deelgraaf geldt dat het chromatisch getal gelijk is aan het cliquegetal.

De Petersen-graaf (Figuur 5) is een voorbeeld van een graaf die *niet* perfect is, omdat het cliquegetal van de graaf zelf verschilt van zijn kleurgetal. Bipartite grafen zijn perfect omdat ze chromatisch getal 2 hebben. We hebben de volgende stelling over de Shannon-capaciteit van perfecte grafen.

**Stelling 2.** *Zij  $G$  een perfecte graaf, dan geldt*

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

Voor het bewijs verwijzen we naar [2, Hoofdstuk 5].



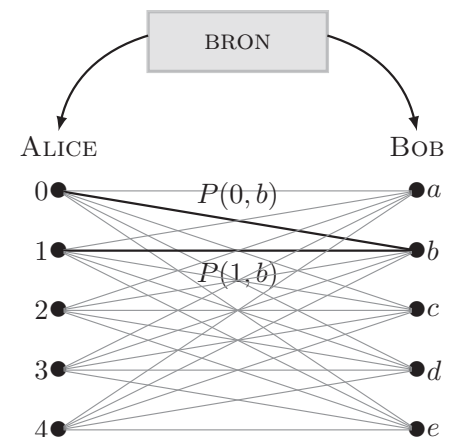
Figuur 5 De Petersen-graaf heeft cliquegetal 2 en chromatisch getal 3.

**Broncodering**

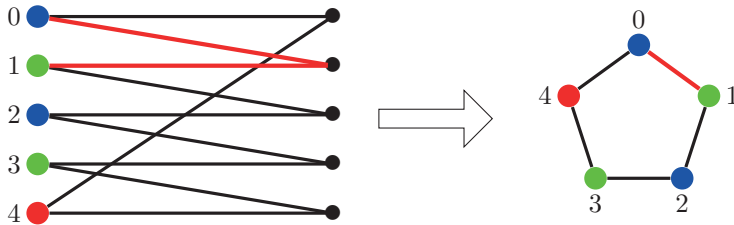
In het broncoderingprobleem krijgen twee partijen, Alice en Bob, allebei een input van een externe bron en is hun doel om met zo min mogelijk communicatie Alices input aan Bob duidelijk te maken. Alice kan hiervoor uiteraard haar hele input naar Bob sturen, maar soms kan er communicatie bespaard worden 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  $P$  onveranderd blijft na elke keer dat de bron inputs uitdeelt.

Zoals Shannon voor het kanaalcoderingprobleem, beschouwde Witsenhausen [10] de minimale communicatie die nodig is in het geval waarin er geen fouten getole-



Figuur 6 Een discrete bron met 5 mogelijke inputs voor Alice en Bob.



**Figuur 7** Van een bron naar zijn karakteristieke graaf.

reerd 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 6 krijgen we zo bijvoorbeeld een graaf die er zo uitziet als die van Figuur 2.

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 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. Zoals voor het kanaalcoderingsprobleem is er voor elke graaf een bron met die graaf als karakteristieke graaf. Om het broncoderingsprobleem op te lossen kijken we echter naar een andere graafparameter dan het onafhankelijkheidsgetal. Het oplossen van een broncoderingsprobleem betekent dat Alice voor elk van haar mogelijke input  $u$  een zo kort mogelijk bericht voor Bob heeft waaruit hij samen met zijn eigen input  $v$  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 broncoderingsprobleem op te lossen. De eerste stelling voor het broncoderingsprobleem luidt dus:

**Stelling 3.** *Het oplossen van één instantie van het broncoderingsprobleem 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.** *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  $u_1, \dots, u_n \in V$  en  $v_1, \dots, v_n \in V$  van Alice niet met zekerheid kan onderscheiden. Merk op dat dit gebeurt wanneer voor elke  $i \in \{1, \dots, n\}$  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 4.** *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 6.** (Witsenhausen-snelheid). De *Witsenhausen-snelheid* van een graaf  $G$  is gedefinieerd als

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

Als de blok lengte 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 6.** *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 negen kleuren voldoende zijn voor  $C_5^{\boxtimes 2}$ .

**Propositie 7** (Witsenhausen).  $\chi(C_5^{\boxtimes 2}) \leq 5$ .

De meest expliciete manier om dit te zien is door te verifiëren dat Witsenhausens kleuring (Figuur 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

(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 8** Witsenhausens kleuring van  $C_5 \boxtimes C_5$ .

$(x,y) - (x',y') \pmod{5}$  behoort tot de verzameling

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

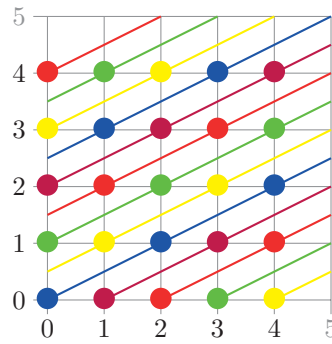
Beeld de knopen van  $C_5^{\boxtimes 2}$  af op een tweedimensionaal grid (Figuur 9).

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 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 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 Witsenhausen-snelheid van  $C_5$ .

**Propositie 8** (Lovász).  $R(C_5) = \sqrt{5}$ .



Figuur 9 Lijnkleuring van  $C_5 \boxtimes C_5$ .

Dit volgt direct uit Stelling 1, 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 9.** Zij  $G = (V,E)$  een graaf. Dan geldt

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

Waarom is dit zo? Stel we hebben een geldige kleuring van een graaf  $G$  met  $c = \chi(G)$  knopen. Noem de kleuren  $1, 2, \dots, c$ . Voor kleur  $i$ , laat  $n_i$  het aantal knopen met kleur  $i$  zijn. Elke knoop heeft een kleur, dus het totale aantal knopen is  $n_1 + n_2 + \dots + n_c = |V|$ . 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.  $\square$

## Referenties

- M. Aigner en G.M. Ziegler, *Proofs from THE BOOK*, Springer, 2014.
- R. Diestel, *Graph Theory*, Graduate Texts in Mathematics, Vol. 173, Springer, 2005.
- J. Körner en A. Orłitsky, Zero-error information theory, *IEEE Trans. Inform. Theory* 44(6), *Information Theory: 1948–1998* (1998) 2207–2229.
- L. Lovász, On the Shannon capacity of a graph, *IEEE Trans. Inform. Theory* 25(1) (1979) 1–7.
- E. Lubetzky, *Graph Powers and Related Extremal Problems*, Ph.D. thesis, Tel Aviv University, 2007.
- K.A. Mathew en P.R.J. Östergård, New lower bounds for the Shannon capacity of odd cycles, *Designs, Codes and Cryptography* 84 (2015), 13–22.
- J. Nayak, E. Tuncel en K. Rose, Zero-error source-channel coding with side information, *Information Theory, IEEE Transactions on* 52(10) (2006), 4626–4629.
- C.E. Shannon, A mathematical theory of communication, *Bell System Technical Journal* 27 (1948), 379–423, 623–656.
- C.E. Shannon, The zero error capacity of a noisy channel, *Institute of Radio Engineers, Transactions on Information Theory* 2(3) (1956), 8–19.
- H.S. Witsenhausen, The zero-error side information problem and chromatic numbers, *IEEE Trans. Information Theory* 22(5) (1976), 592–593.