Discrete Wiskunde

Bert De Saffel

2017-2018

Inhoudsopgave

Samenvatting

Deze tekst vat de theorie van Discrete Wiskunde samen zoals die gegeven werd in het academiejaar 2017-2018.

Deel I

Discrete Wiskunde

Hoofdstuk 1

Eindige Velden

1.1 Proloog

_TODO: veel korter schrijven Vooraleer velden kunnen uitgelegd worden moet eerst de inleiding van hoofdstuk 2.5.3 (Groepen) gegeven worden.

- **Groep** (symbool = **G**): Een verzameling elementen die elk met elkaar onderling interageren.
- **Groepstabel**: Een matrix dat interacties voorstelt.

Ter opmerking, het symbool $\oplus$ stelt het additieve voor en $\otimes$ stelt het multiplicatieve voor. Dit is een hulpmiddel voor ons zodat we kunnen vergelijken met de + en . operator uit de wiskunde. Er zijn 4 eigenschappen nodig om een geldige groepstabel te hebben.

- **Inwendigheid**: x $\oplus$ y = element van G
- **Associativiteit**: (a $\oplus$ b) $\oplus$ c = a $\oplus$ (b $\oplus$ c)
- **Neutraal Element (n)**: x $\oplus$ n = x
- **Invers element**: x $\oplus$ $\overline{x}$ = **n**

Een extra, maar niet verplichte eigenschap is **Commutativiteit**. x $\oplus$ y = y $\oplus$ x.

Enkele begrippen met betrekking tot groepstabel.

Tabel 1.1: Een groepstabel voor de interactie ‘optellen’ in modulo 12

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

- **Latijns Vierkant**: Een groepstabel waarvan elk element exact één keer voorkomt in elke rij en kolom (denk aan Sudoku).

- **Isomorfe groepen**: Verschillende groepen die niets met elkaar te maken hebben kunnen isomorf zijn. Dit betekent dat ze identiek zijn na eventuele herlabeling of permutaties van kolommen of rijen.

- **Discrete groepen**: Dit zijn groepen met een eindig aantal elementen. Modulo 12 heeft zo 12 elementen.

- **De orde**: Enerzijds is dit getal het aantal elementen van een groep. Anderzijds is dit het aantal keer dat je een element met zichzelf moet laten interageren om het neutraal element te bekomen. De orde is dus voor elk element verschillend.

Als je de verzameling ’Modulo 12’ bekijkt heb je 12 elementen. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 en 11.

* Hoeveel keer moet je 1 met zichzelf optellen om 0 te bekomen? (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0)$\rightarrow$ 12

* Hoeveel keer moet je 2 met zichzelf optellen om 0 te bekomen? (2, 4, 6, 8, 10, 0) $\rightarrow$ 6

* Hoeveel keer moet je 5 met zichzelf optellen om 0 te bekomen? (5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0) $\rightarrow$ 12

De orde van 1 is dus 12, die van 2 is 6 en die van 5 is ook 12.

- **Generator**: Een element of een combinatie van elementen die, als je die met elkaar laat interageren, alle andere elementen van de groep tegenkomt. In de vorige voorbeelden kan je zien dat zowel 1 als 5 een generator zijn aangezien ze elk element tegenkomen. Je kan ook elementen combineren om een generator te vormen. Zo is $< 2, 3 >$ ook een generator want $(2 + 2 + 3 + 3 + 3) \mod 12 = 1$.

Tot nu toe hebben we enkel additieve groeptabellen gezien. In tabel 1.1 kan je zien dat de groep Modulo 12 voor de bewerking $\oplus$ een discrete groep is

Multiplicatie is geen groepstabel tenzij we de 0 uitsluiten en als de groep n aantal element bevat waarbij n een priemgetal is. Dit wordt duidelijk gemaakt in het onderdeel Priemvelden

Een cyclische groep is een groep dat slechts 1 element heeft als generator.
$i = (29w^i)\%36$
29 = invers element via algemeen algoritme van euclides

1.2 Priemvelden

Priemvelden is een eerste methode om een cyclische groep te vinden van een bepaalde orde.

- **Veld**: Verzameling F van elementen {a, b, c, ...} die onderling interageren via een interactie $\oplus$ en via een interactie $\otimes$.

- **Veldaxioma's**

  1. (F, $\oplus$) $\rightarrow$ Een additieve groep met neutraal element **0** (**nul**element)
  2. (F\0 , $\otimes$) $\rightarrow$ Multiplicatieve groep met neutraal element **1** (**eenheids**element)
  3. Distributieve eigenschap: a $\otimes$ (b $\oplus$ c) = (a $\otimes$ b) $\oplus$ (a $\otimes$ c)

- **Eindig veld**: Veld met eindig aantal element n

- Voor elke orde n is er maximum één enkel eindig veld met orde n

- De multiplicatieve groep (F\0 , ⊗) van een eindig veld (F, ⊕ , ⊗) is cyclisch

Hoe kan het veld met orde n geconstrueerd worden met groepstabellen (F, ⊕) en (F, ⊗)? → Alle eindige velden kunnen met behulp van één van twee methodes geconstrueerd worden.

(Z_p, +, .) vormt een veld met nulelement **0** en eenheidselement **1** op voorwaarde dat p een priemgetal is. Dit heet een **priemveld**. Hieruit volgt dat (Z_p\0, .) een cyclische groep is indien p een priemgetal is.

1.2.1 Priemontbinding

_TODO: todo

1.2.2 Algoritme van Euclides

- Numerieke uitwerking van het **algoritme van Euclides**:

99		
-84	**1** (84 kan **1** keer in 99 99 - 84 = 15)	84
15	**5** (15 kan **5** keer in 84)	-75
-9	1 (1 keer in 15 = 1 * 9)	9
6	1 (1 keer in 9 = 1 * 6)	-6
-6	2	3
0		

pi = 3 + 1/(7 + 1/(15))...

1.2.3 Multiplicatieve functies

Euler ϕ

Definitie: Hoeveel getallen kleiner dan x zijn priemgetallen?
Voorbeeld: $90 = 2 * 3^2 * 5$
$\phi(90) = 90 * (1/2) * (2/3) * (4/5) =$ **24**

1.2.4 Möbius μ

Heeft 3 uitkomsten: -1, 0 of 1.

- **0**: Minstens één van de priemfactoren komt meer dan 1 keer voor.
- **-1**: Oneven aantal priemfactoren
- **1**: Even aantal priemfactoren
- $\mu(35) = 1$, want $5 * 7 = evenaantalpriemfactoren$

Möbius Inversie:

- Wordt gebruikt om $\phi(x)$ te berekenen.
- $\phi(x) = \mu(1) * (90/1)$
  $+ \mu(2) * (90/2)$
  $+ \mu(3) * (90/3)$
  $+ \mu(5) * (90/5)$
  $+ \mu(10) * (90/10)$
  $+ \mu(15) * (90/15)$
  $+ \mu(30) * (90/30)$

1.2.5 Primitieve wortels

Interacties met zichzelf om uiteindelijk 1 uit te komen. Bij de primitieve wortel moet je de *orde* aantal keer interageren met zichzelf om 1 uit te komen
stel $p = 601$ $600 =$ aantal elementen $600 = 2^3 * 3 * 5^2$
rooster opstellen *TODO: rooster* $8{*}3{*}25 = 600$ is het enige dat als uitkomst 1 mag hebben, zonder computer kan je best enkel de laatste aansluitingen controleren

1.2.6 Discrete logaritmen

Bepaal index i van het getal x van verzameling p met primitieve wortel w
VB: $p = 401, w = 3, i = 13$

1.2.7 Naïve methode

1.2.8 Baby-step Giant-step

1.3 Galoisvelden

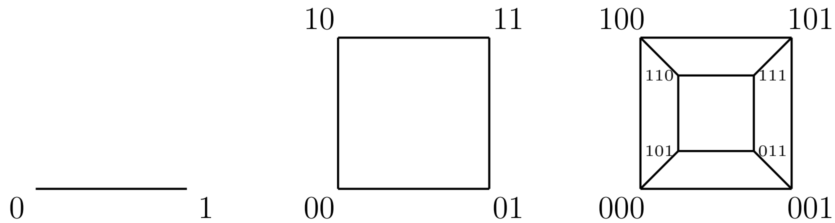
Hoofdstuk 2

Grafen

2.1 Terminologie

- **Graad** van een knoop: aantal buren van een knoop.
- Aantal **bogen**: de helft van de som van de graden van alle knopen.
- δ: De kleinste graad in een graaf.
- Δ: De grootste graad in een graaf.
- Een graaf is **regulier** als $\delta = \Delta$.
- Een graaf is **compleet** als elke knoop met elke andere knoop is verbonden.
- **Cykelgraaf**: Een graaf waarbij elke knoop 2 buren heeft.
- **Wandelen**: Van knoop naar knoop gaan.
- **Pad**: Elk knooppunt mag maar één keer in een wandeling voorkomen.
- **Brug**: Een boog dat 2 grafen verbindt.
- **Gerichte graaf**: Graaf waar de bogen een richting hebben.
- **Gewogen graaf**: Graaf waar elke boog een kost heeft.
- **Subgraaf**: Een graaf G" waarvan de knopen - en bogenverzameling een deelverzameling is van een graaf G'.

- **Isomorfe graaf**: Een graaf G” die, als je knopen en bogen verlegt, overeen komt met graaf G’.
- **Bipartiete graaf**: De graaf is gepartitioneerd in partities. Enkel bogen tussen partities zijn mogelijk.
- **Complete Bipartiete graaf**: Elke knoop van één partitie is verbonden met elke knoop uit de andere partitie.
- **Kubus**: Een bipartiete graaf met 2^n knopen, binair geïdentificeerd, met bogen tussen knopen waarvan de identificatie 1 bit verschilt.



2.2 Connectiviteit

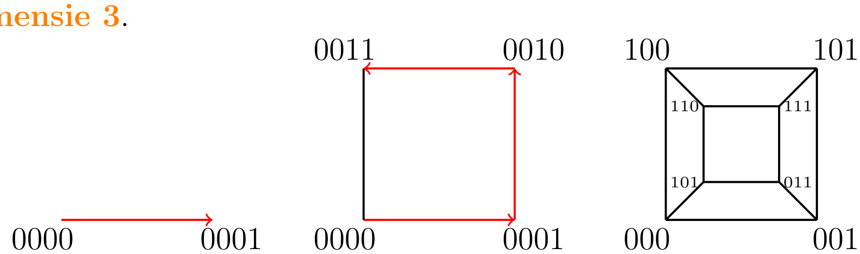
2.2.1 Eulercircuit - Niet kennen

Elke boog mag maar één keer in een wandeling voorkomen.

2.2.2 Hamiltoncircuit

Elk knooppunt mag maar één keer in een wandeling voorkomen. Hier gelden twee voorwaarden (**Niet te kennen**)

De **Gray Code** is een Hamiltoncircuit in een kubus. Zie slide 30 van 2a.pptx. Op het examen komt dit in de vorm : **Geef gray code van een dimensie 3**.



In excel *TODO: ...* : $\begin{array}{c} 000\mathbf{0} \\ 000\mathbf{1} \\ \hline 001\mathbf{1} \\ 001\mathbf{0} \\ \hline 0110 \\ 0111 \\ 0101 \\ 0100 \\ \hline 1100 \\ 1101 \\ 1111 \\ 1110 \\ 1010 \\ 1011 \\ 1001 \\ 1000 \end{array}$

2.2.3 Boogconnectiviteit Niet kennen

2.2.4 Knoopconnectiviteit

De knoopconnectiviteit is het aantal elementen in de kleinste knoopsnede van een graaf. Een knoopsnede is een soort brug dat bestaat uit meerdere knopen. Als deze knoopsnede verwijderdt wordt uit de graaf is de graaf niet meer samenhangend, maar bestaat dan uit 2 grafen. Voor een willekeurige samenhangende graaf : $K \leq \lambda \leq \delta$. zie slides pls

2.3 Matrixvoorstellingen

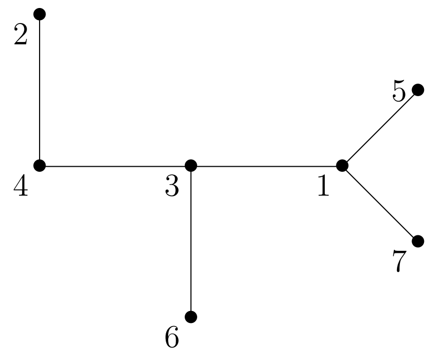
2.3.1 Adjacant ("Waardeloos" - Moreau)

2.3.2 Incidentiematrix

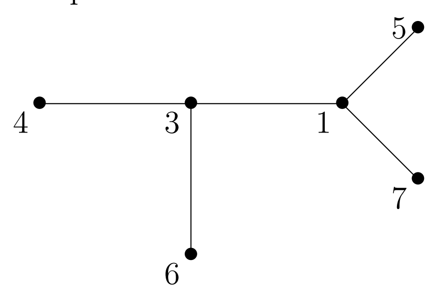
2.4 Bomen

2.4.1 Examenvraag 1: Identificeer een boom volgens Prüfers methode

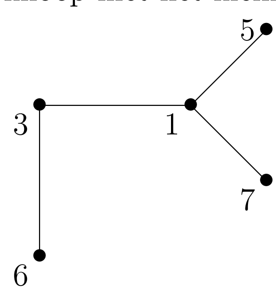
De knoop met het kleinste label en slechts één buurt heeft verwijderen en het label opschrijven aan welke knoop deze knoop vasthangde. Het eindresultaat moeten 2 knopen zijn.



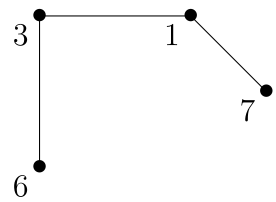
De knoop met het kleinste label is **2** en hangt vast aan **4**. $\sigma = 4$



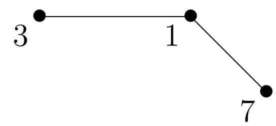
De knoop met het kleinste label is **4** en hangt vast aan **3**. $\sigma = 4, 3$



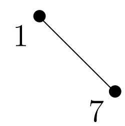
De knoop met het kleinste label is **5** en hangt vast aan **1**. $\sigma = 4, 3, 1$



De knoop met het kleinste label is **6** en hangt vast aan **3**. $\sigma = 4, 3, 1, 3$



De knoop met het kleinste label is **3** en hangt vast aan **1**. $\sigma = 4, 3, 1, 3, 1$



2 knopen resterend. Eindresultaat: $\sigma = 4, 3, 1, 3, 1$

2.4.2 Examenvraag 2: Teken een boom volgens Prüfers methode

$\sigma = 4, 3, 1, 3, 1$
$S = 1, 2, 3, 4, 5, 6, 7$
TODO: uitwerken 2 komt niet voor in σ, 4$\rightarrow$ 2
4 komt niet voor in σ 3$\rightarrow$4

2.4.3 Binaire boom

Een hiërarchische boom waar op elk niveau maximaal 2 aftakkingen mogelijk zijn. Het **Catalan** getal zegt hoeveel bomen er zijn met n aantal knopen.

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

2.5 Bipartiete matching

Matching in een bipartiete graaf wil zeggen dat je een deelverzameling overhoudt zodat er voor elke knoop maximaal één verbinding is. Het is geen voorwaarde dat alle knopen een verbinding moeten hebben.

2.5.1 Volledige matching

Een volledige matching is een matching waarbij elke knoop precies één verbinding heeft. De **Stelling van Hall** zegt dat een bipartiete graaf een volledige matching heeft als de **deficiëntie** μ nul is. De deficiëntie is een getal dat het verschil van het aantal knopen tussen de twee grafen van een bipartiete graaf voorstelt. Stel dat de graaf X 4 knopen heeft en Y 5 knopen, dan is er eenheids deficit van 1. De stelling van Hall is hier dus niet geldig.

2.5.2 Maximale matching

Als een volledige matching niet mogelijk is (stelling van Hall), dan kan er nog altijd een optimale matching gezocht worden.
Hongaars algoritme:

- Trek intuitief een aantal paden
- Verwissel stippellijnen met volle lijnen en omgekeerd (*_TODO: wtf*)
- Vanaf er geen stippellijnen zijn is er een maximale matching bereikt.

2.5.3 Stabiele matching

Stabiele matching heeft betrekking tot complete bipartiete grafen. Dit wil zeggen dat elke boog gericht zijn en een gewicht hebben.
Gale-Shapley algoritme: Vrij eenvoudig. Zie slide 8 van 2c.pptx