

## Inhoudsopgave

<b>1</b>	<b>Recurrente betrekkingen</b>	<b>3</b>
1.1	De torens van Hanoi . . . . .	3
1.2	Vlakverdeling . . . . .	7
1.3	Het Josephus-probleem . . . . .	9
<b>2</b>	<b>Recurrente betrekkingen</b>	<b>12</b>
2.1	Fibonacci . . . . .	12
2.2	Euclides . . . . .	15
2.3	AVL . . . . .	16
2.4	Mergesort . . . . .	17
2.5	Algemene oplossing . . . . .	20
<b>3</b>	<b>Sommatie</b>	<b>22</b>
3.1	De sigma-notatie . . . . .	22
3.2	Sommatiefactor . . . . .	23
3.3	Quicksort . . . . .	24
3.4	Rekenregels . . . . .	26
<b>4</b>	<b>Differentierekening en reeksen</b>	<b>31</b>
4.1	Delta . . . . .	31
4.2	Differentie-sommatiestelling . . . . .	32
4.3	Analoga . . . . .	34
4.4	Reeksen . . . . .	36
<b>5</b>	<b>Afronden en afkappen</b>	<b>40</b>
5.1	Floor en ceiling . . . . .	40
5.2	Geheeltallige deling . . . . .	45
5.3	Sommatie . . . . .	46
<b>6</b>	<b>Complexe getallen</b>	<b>48</b>
6.1	Definitie . . . . .	48
6.2	Rekenregels . . . . .	49
6.3	Poolcoördinaten . . . . .	50
6.4	Nulpunten . . . . .	52
<b>7</b>	<b>Deelbaarheid</b>	<b>56</b>
7.1	Deelbaarheid . . . . .	56
7.2	Priemgetallen . . . . .	57
7.3	Congruenties . . . . .	61

7.4	Euler . . . . .	61
7.5	RSA . . . . .	63
<b>8</b>	<b>Vectoren</b>	<b>64</b>
8.1	Vectoren . . . . .	64
8.2	Lineaire combinaties . . . . .	65
8.3	Lijn en vlak . . . . .	67
8.4	Norm en inproduct . . . . .	68
<b>9</b>	<b>Matrixrekening</b>	<b>72</b>
9.1	Vergelijkingen . . . . .	72
9.2	Matrixvermenigvuldiging . . . . .	73
9.3	Determinant . . . . .	74
9.4	Lineaire afbeeldingen . . . . .	80
9.5	Eigenwaarden . . . . .	81
<b>10</b>	<b>Binomiaalcoëfficiënten</b>	<b>81</b>
10.1	Definitie . . . . .	81
10.2	Identiteiten . . . . .	83
10.3	De binomiaalstelling . . . . .	85
10.4	Producten . . . . .	87
10.5	Newtonreeksen . . . . .	88
<b>11</b>	<b>Voortbrengende functies</b>	<b>90</b>
11.1	Repertoire . . . . .	90
11.2	Convolutie . . . . .	93
11.3	Recurrente betrekkingen . . . . .	95
11.4	Goedhaakse expressies . . . . .	97
<b>12</b>	<b>Kansrekening</b>	<b>99</b>
12.1	Kansruimten . . . . .	99
12.2	Variantie . . . . .	102
12.3	Kansvoortbrengende functies . . . . .	107
<b>13</b>	<b>Asymptotiek</b>	<b>108</b>
13.1	Asymptotiek . . . . .	108
13.2	Reeksontwikkelingen . . . . .	111
13.3	O-manipulatie . . . . .	112
13.4	Bootstrapping . . . . .	114
<b>14</b>	<b>Grafen</b>	<b>117</b>

14.1 Grafen . . . . .	117
14.2 Paden . . . . .	120
14.3 Bomen . . . . .	121
14.4 Planariteit . . . . .	122

## 1 Recurrente betrekkingen

### 1.1 De torens van Hanoi

#### De torens van Hanoi



Edouard Lucas, 1884:

- Gegeven 3 pinnen en 64 schijven van verschillende grootte.
- Startsituatie: 64 op linkerpin, geordend naar grootte.
- Opgave: verplaats ze alle naar rechterpin.
- Regel 1: er mag maar 1 schijf tegelijk worden verplaatst.
- Regel 2: nooit mag een grotere schijf rusten op een kleinere.

#### Generalisatie en naamgeving

- Generalisatie: beschouw het geval met  $n$  schijven.
- Naamgeving: zij  $T_n$  het minimale aantal bewegingen dat het probleem oplost.
- Beschouw kleine gevallen:  $T_0 = 0$ ,  $T_1 = 1$ ,  $T_2 = 3$ .

#### Recurrente betrekking

Stel dat we weten hoe we  $n - 1$  schijven kunnen verplaatsen, kunnen we het dan ook met  $n$ ?

- Observatie: als de grootste schijf wordt verplaatst, kan dat alleen naar een lege pin.

- Het bereiken van die toestand kost op zijn zuinigst  $T_{n-1}$  verplaatsingen.
- Daarna moeten de  $n - 1$  overige schijven worden verplaatst.
- Dat kost ook minimaal  $T_{n-1}$  stappen.

Conclusie:

$$T_n = 2T_{n-1} + 1 \quad \text{voor } n > 0$$

dus  $T_0 = 0, T_1 = 1, T_2 = 3, T_3 = 7, T_4 = 15, T_5 = 31, \dots$

## Programma

### Java-methode die $n$ schijven verplaatst

```
void move(n, Pin source, Pin destination, Pin auxiliary)
{ if (n > 0)
  { move(n-1, source, auxiliary, destination);
    moveOne(source, destination);
    move(n-1, auxiliary, destination, source);
  }
}
```

Dit is de efficiëntst mogelijke methode (in aantal verplaatsingen). Het genereerde aantal verplaatsingen is  $T_n$ , de (tijd)complexiteit van dit programma is daarmee evenredig.

Merk op: dit is een recursieve methode, een methode die zichzelf aanroept. Zorg ervoor dat zo iets niet tot een oneindige reeks aanroepen leidt. Dat gaat hier goed omdat  $0 \leq n-1 < n$ .

### Output voor $n = 8$

1. Verplaats schijf van links naar rechts 2. Verplaats schijf van links naar midden 3. Verplaats schijf van rechts naar midden 4. Verplaats schijf van links naar rechts 5. Verplaats schijf van midden naar links 6. Verplaats schijf van midden naar rechts 7. Verplaats schijf van links naar rechts 8. Verplaats schijf van links naar midden 9. Verplaats schijf van rechts naar midden 10. Verplaats schijf van rechts naar links ... 250. Verplaats schijf van rechts naar links 251. Verplaats schijf van midden naar links 252. Verplaats schijf van rechts naar midden 253. Verplaats schijf van links naar rechts 254. Verplaats schijf van links naar midden 255. Verplaats schijf van rechts naar midden

## Vermoeden

### Java-methode die $T_n$ uitrekent

```
int T(int n)
{ if (n==0) return 0;
  return 2*T(n-1)+1;
}
```

Dit programma berekent  $T_n$  door middel van de recurrente betrekking:  $T_0 = 0$ ,  $T_n = 2T_{n-1} + 1$  voor  $n > 0$ . De output is: 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767, 65535, 131071, 262143, 524287, ...

Vermoeden:

$$T_n = 2^n - 1 \quad \text{voor } n \geq 0$$

Hoe kunnen we nagaan of dit inderdaad altijd waar is?

### Inductiebewijs

Een algemene manier om te bewijzen dat een zekere uitspraak  $P_n$  geldt voor alle  $n$  met  $n \geq 0$ , bestaat uit twee onderdelen:

1. Basis: Bewijs dat  $P_0$  geldt.
2. Stap: Bewijs dat voor elke  $n$  met  $n > 0$  waarvoor  $P_{n-1}$  geldt ook  $P_n$  geldt.

In ons geval is  $P_n$  de uitspraak  $T_n = 2^n - 1$ . Er geldt

$$\begin{aligned} T_0 &= \{ \text{recurrente betrekking} \} \\ &= 0 \\ &= \{ \text{rekenen} \} \\ &= 2^0 - 1 \end{aligned}$$

waarmee we de basis hebben bewezen.

### Inductiestap

Neem aan  $n > 0$  en  $T_{n-1} = 2^{n-1} - 1$  (de inductiehypothese). Dan

$$\begin{aligned} T_n &= \{ \text{recurrente betrekking} \} \\ &= 2T_{n-1} + 1 \\ &= \{ \text{inductiehypothese} \} \\ &= 2(2^{n-1} - 1) + 1 \\ &= \{ \text{rekenen} \} \\ &= 2^n - 1 \end{aligned}$$

dus we hebben ook de inductiestap bewezen. Conclusie:

$$T_n = 2^n - 1 \quad \text{voor } n \geq 0$$

**Hint calculus**

Manier van opschrijven van wiskundige bewijzen, geïntroduceerd door de informatici Edsger W. Dijkstra en Wim Feijen rond 1980. Ook erg geschikt voor het construeren van (vooral functionele) programma's.

Bewijs dat  $A = D$  door een afleiding van de vorm

$$\begin{aligned}
 & A \\
 = & \quad \{ \text{uitleg waarom } A = B \} \\
 & B \\
 = & \quad \{ \text{uitleg waarom } B = C \} \\
 & C \\
 = & \quad \{ \text{uitleg waarom } C = D \} \\
 & D
 \end{aligned}$$

Dit werkt ook voor langere bewijzen en voor relaties zoals  $\geq$  of  $\Rightarrow$ . Voordeel: de lezer hoeft de uitleg niet zelf te verzinnen, en er wordt expliciet waar welk gegeven is gebruikt.

**Alternatief bewijs: coördinatentransformatie**

Introduceer de notatie  $U_n = T_n + 1$ . Dan  $U_0 = 1$  en voor  $n > 0$

$$\begin{aligned}
 & U_n \\
 = & \quad \{ \text{definitie van } U_n \} \\
 & T_n + 1 \\
 = & \quad \{ \text{recurrente betrekking voor } T_n \} \\
 & (2T_{n-1} + 1) + 1 \\
 = & \quad \{ \text{rekenen} \} \\
 & 2(T_{n-1} + 1) \\
 = & \quad \{ \text{definitie van } U_n \} \\
 & 2U_{n-1}
 \end{aligned}$$

Dus voor  $n > 0$  is  $U_n = 2U_{n-1}$ . Daaruit zien we meteen in dat

$$U_n = 2^n \quad \text{voor } n \geq 0$$

Moraal: gebruik geschikte coördinaten.

**Mathematica**

Invoer:

```
RSolve[{T[n] == 2T[n - 1] + 1, T[0] == 0}, T[n], n]
```

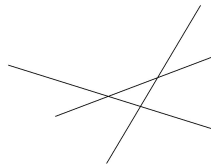
Uitvoer:

```
{{T[n] -> -1 + 2^n}}
```

## 1.2 Vlakverdeling

### Vlakverdeling met rechte lijnen

Jacob Steiner, 1826: In hoeveel delen kan het platte vlak worden verdeeld door middel van een gegeven aantal rechte lijnen?



Naamgeving: Noem het grootste aantal stukken dat met  $n$  lijnen kan worden gemaakt  $L_n$ .

Kleine gevallen:  $L_0 = 1$ ,  $L_1 = 2$ ,  $L_2 = 4$ .

Eerste vermoeden:  $L_n = 2^n$ . Helaas:  $L_3 = 7$ .

### Recurrente betrekking

Stel er zijn al  $n - 1$  lijnen getekend. Het tekenen van de  $n$ -de lijn vergroot het aantal stukken maximaal als die alle voorgaande lijnen snijdt. Dit kunnen we inderdaad bereiken, door deze niet evenwijdig aan de voorgaande te kiezen. Er worden dan  $n$  nieuwe vlakdelen afgesneden.

Conclusie:

$$L_0 = 1$$

$$L_n = L_{n-1} + n \quad \text{voor } n > 0$$

### Vermoeden

$$\begin{aligned} L_n &= \{ \text{recurrente betrekking} \} \\ &= L_{n-1} + n \\ &= \{ \text{recurrente betrekking} \} \\ &= L_{n-2} + (n-1) + n \\ &= \{ \text{recurrente betrekking} \} \\ &= L_{n-3} + (n-2) + (n-1) + n \\ &= \{ \text{recurrente betrekking} \} \\ &\vdots \\ &= \{ \text{recurrente betrekking} \} \\ &= L_0 + 1 + 2 + \dots + (n-2) + (n-1) + n \\ &= \{ L_0 = 1; \text{noteer } S_n = 1 + \dots + n \} \\ &= 1 + S_n \end{aligned}$$

**Vermoeden**

Het voorgaande is niet echt een bewijs, omdat we het gebruik van stippeltjes niet kunnen vermijden. In wezen is dit een analogieredenering!

(Valkuil: wat is de graad van het polynoom  $(x - a)(x - b) \cdots (x - z)$ ?)

De redenering leidt wel tot het sterke vermoeden dat

$$L_n = 1 + S_n \text{ voor } n \geq 0$$

waar  $S_n$  het  $n$ de driehoeksgetal  $1 + \cdots + n$  is.

**Driehoeksgetallen**

Argument van Carl Friedrich Gauss (1786, 9 jaar oud!):

$$\begin{aligned} S_n &= \text{\{per definitie\}} \\ &= 1 + 2 + \cdots + (n - 1) + n \\ &= \text{\{verdubbeling\}} \\ &= \frac{1}{2}((1 + 2 + \cdots + (n - 1) + n) + (1 + 2 + \cdots + (n - 1) + n)) \\ &= \text{\{omkering volgorde in de tweede helft\}} \\ &= \frac{1}{2}((1 + 2 + \cdots + (n - 1) + n) + (n + (n - 1) + \cdots + 2 + 1)) \\ &= \text{\{twee aan twee samennemen van termen\}} \\ &= \frac{1}{2}((1 + n) + (2 + (n - 1)) + \cdots + ((n - 1) + 2) + (n + 1)) \\ &= \text{\{in totaal } n \text{ termen, die alle } n + 1 \text{ groot zijn\}} \\ &= \frac{1}{2}n(n + 1) \end{aligned}$$

Ook dit is nog geen echt bewijs (stippeltjes), maar het kan daartoe wel worden omgevormd als we sommen ( $\sum_{k=1}^n$ ) in ons repertoire van standaardoperaties opnemen. Dan zijn wel rekenregels voor 'omkeren' en 'samennemen' nodig. Zie volgend college!

**Inductiebewijs**

Vermoeden:

$$L_n = 1 + \frac{1}{2}n(n + 1)$$

Basis:  $L_0 = 1$  en ook  $1 + \frac{1}{2}0(0 + 1) = 1$ .

Stap: neem aan  $n > 0$  en  $L_{n-1} = 1 + \frac{1}{2}(n - 1)n$  (inductiehypothese). Dan

$$\begin{aligned} L_n &= \text{\{recurrente betrekking\}} \\ &= L_{n-1} + n \\ &= \text{\{inductiehypothese\}} \\ &= 1 + \frac{1}{2}(n - 1)n + n \\ &= \text{\{haal factor } \frac{1}{2}n \text{ buiten haakjes\}} \\ &= 1 + \frac{1}{2}n(n - 1 + 2) \\ &= \text{\{rekenen\}} \\ &= 1 + \frac{1}{2}n(n + 1) \end{aligned}$$

**Conclusie**

Hiermee is echt bewezen dat

$$L_n = 1 + \frac{1}{2}n(n+1) \quad \text{voor } n \geq 0$$

Gevolg:

$$L_n \approx \frac{1}{2}n^2 \quad \text{voor grote waarden van } n$$

**Mathematica**

Invoer:

```
RSolve[{L[n] == L[n - 1] + n, L[0] == 1}, L[n], n]
```

Uitvoer:

$$\{\{L[n] \rightarrow \frac{1}{2}(2 + n + n^2)\}\}$$

**1.3 Het Josephus-probleem****Het Josephus-probleem**

Flavius Josephus (ca. 37-100), Joods geschiedschrijver van de oorlog tegen de Romeinen: 41 personen staan in een cirkel. Elke tweede wordt gedood totdat er maar één over is. Vraag: wie is de laatste overlevende?

Beschouw het algemene probleem voor  $n$  personen, voor  $n \geq 1$ . Zij  $J(n)$  het nummer van de laatste overlevende. (We schrijven  $J(n)$  in plaats van  $J_n$  omdat we straks een ingewikkelde expressie als index krijgen. Dit vereist helderziendheid...)

Kleine gevallen:  $J(1) = 1$ ,  $J(2) = 1$ ,  $J(3) = 3$ ,  $J(4) = 1$ ,  $J(5) = 3$ ,  $J(6) = 5$ , ... Er dient zich geen vermoeden aan.

Het valt op dat  $J(n)$  altijd oneven lijkt te zijn. Reden: alle mannen met even nummer zijn gedood in de eerste rondgang.

**Recurrente betrekking**

Hoe is de situatie na de eerste rondgang? Beschouw het geval  $n = 2k$ . Nog in leven zijn de nummers  $1, 3, 5, \dots, 2k - 1$ . Dat is gelijk aan de uitgangssituatie met  $k$  personen maar met elk nummer  $t$  vervangen door  $2t - 1$ , dus het nummer van de laatste overlevende is  $2J(k) - 1$ .

Beschouw het geval  $n = 2k + 1$ . Nog in leven zijn de nummers  $3, 5, 7, \dots, 2k + 1$ . Dat is gelijk aan de uitgangssituatie met  $k$  personen, maar met elk nummer  $t$  vervangen door  $2t + 1$ , dus het nummer van de laatste overlevende is  $2J(k) + 1$ .

Recurrente betrekking:

$$\begin{aligned} J(1) &= 1 \\ J(2k) &= 2J(k) - 1 \quad \text{voor } k \geq 1 \\ J(2k + 1) &= 2J(k) + 1 \quad \text{voor } k \geq 1 \end{aligned}$$

(Mathematica ondersteunt vergelijkingen van dit type niet!)

### Programma

#### Java-methode die $J(n)$ uitrekent

```
int J(int n)
{ if (n==1) return 1;
  int k = n/2;
  if (n%2==0) return 2*J(k)-1;
  return 2*J(k)+1;
}
```

Merk op dat dit programma heel efficiënt is: per aanroep wordt het argument van  $J$  minstens gehalveerd.

### Vermoeden

Uitvoer:

$J(1) = 1,$   
 $J(2) = 1, J(3) = 3,$   
 $J(4) = 1, J(5) = 3, J(6) = 5, J(7) = 7,$   
 $J(8) = 1, J(9) = 3, J(10) = 5, J(11) = 7,$   
 $J(12) = 9, J(13) = 11, J(14) = 13, J(15) = 15,$   
 $J(16) = 1, J(17) = 3, J(18) = 5, J(19) = 7, \dots$

Vermoeden:

$$J(n) = 2l + 1 \quad \text{waar } n = 2^m + l \text{ en } 0 \leq l < 2^m$$

### Bewijs met inductie

De recurrente betrekking was

$$\begin{aligned}
 J(1) &= 1 \\
 J(2k) &= 2J(k) - 1 \quad \text{voor } k \geq 1 \\
 J(2k + 1) &= 2J(k) + 1 \quad \text{voor } k \geq 1
 \end{aligned}$$

We bewijzen het vermoeden

$$J(n) = 2l + 1 \quad \text{waar } n = 2^m + l \text{ en } 0 \leq l < 2^m$$

met inductie naar  $m$ .

Basis: ingeval  $m = 0$  geldt  $l = 0$  en dus  $n = 1$ ; de uitspraak reduceert tot  $J(1) = 1$ , wat uit de recurrente betrekking volgt.

**Bewijs met inductie**

De recurrente betrekking was

$$\begin{aligned} J(1) &= 1 \\ J(2k) &= 2J(k) - 1 \quad \text{voor } k \geq 1 \\ J(2k+1) &= 2J(k) + 1 \quad \text{voor } k \geq 1 \end{aligned}$$

Stap: zij  $m > 0$  en  $J(n) = 2l + 1$  voor  $n = 2^{m-1} + l$  en  $0 \leq l < 2^{m-1}$ . Zij nu  $n = 2^m + 2p$  met  $0 \leq p < 2^{m-1}$ . Dan

$$\begin{aligned} &J(n) \\ = &\{ n = 2^m + 2p \} \\ &J(2^m + 2p) \\ = &\{ \text{recurrente betrekking met } k = 2^{m-1} + p \} \\ &2J(2^{m-1} + p) - 1 \\ = &\{ \text{inductiehypothese met } l = p \} \\ &2(2p + 1) - 1 \\ = &\{ \text{rekenen} \} \\ &2(2p) + 1 \end{aligned}$$

Hiermee is de stap bewezen voor even  $n$ .

**Bewijs met inductie**

De recurrente betrekking was

$$\begin{aligned} J(1) &= 1 \\ J(2k) &= 2J(k) - 1 \quad \text{voor } k \geq 1 \\ J(2k+1) &= 2J(k) + 1 \quad \text{voor } k \geq 1 \end{aligned}$$

We veronderstellen nog steeds  $m > 0$  en  $J(n) = 2l + 1$  voor  $n = 2^{m-1} + l$  en  $0 \leq l < 2^{m-1}$  en beschouwen nu een oneven  $n$ , zeg  $n = 2^m + (2p + 1)$  met  $0 \leq p < 2^{m-1}$ . Dan

$$\begin{aligned} &J(n) \\ = &\{ n = 2^m + 2p + 1 \} \\ &J(2^m + 2p + 1) \\ = &\{ \text{recurrente betrekking met } k = 2^{m-1} + p \} \\ &2J(2^{m-1} + p) + 1 \\ = &\{ \text{inductiehypothese met } l = p \} \\ &2(2p + 1) + 1 \end{aligned}$$

Hiermee is de stap ook bewezen voor oneven  $n$ .

**Alternatief bewijs zonder rekenen**

1. Als  $n$  even is, dan is na de eerste rondgang het aantal personen gehalveerd en persoon 1 nog in leven.
2. Dus als  $n$  een macht van 2 is, zeg  $2^m$ , dan is na  $m$  rondgangen het aantal personen gereduceerd tot 1 en persoon 1 nog in leven.

3. Zij nu  $n = 2^m + l$  met  $0 \leq l < 2^m$ . Na  $l$  dodingen zijn er  $2^m$  personen nog in leven, en we zijn in de rondgang gekomen tot aan nummer  $2l+1$ . Door hernoeming blijkt dat deze in leven blijft.

### Binaire representatie

We hebben nu bewezen

$$J(n) = 2l + 1 \quad \text{waar } n = 2^m + l \text{ en } 0 \leq l < 2^m$$

In de computer worden getallen binair gerepresenteerd. Noteer

$$n = (b_m b_{m-1} \dots b_1 b_0)_2$$

als afkorting voor

$$n = b_m 2^m + b_{m-1} 2^{m-1} + \dots + b_1 2 + b_0$$

waar elke  $b_i$  de waarde 0 of 1 heeft, en  $b_m = 1$ . Dan

$$n = (1b_{m-1}b_{m-2} \dots b_1b_0)_2$$

$$l = (0b_{m-1}b_{m-2} \dots b_1b_0)_2$$

$$2l = (b_{m-1}b_{m-2} \dots b_1b_0)_2$$

Dus  $2l$  is de zogenaamde left-shift van  $n$ .

## 2 Recurrente betrekkingen

### 2.1 Fibonacci

#### De getallen van Fibonacci

Fibonacci (= Leonardo van Pisa), 1202: Bereken het aantal paren konijnen na één jaar, als

1. er na 1 maand 1 paar pasgeboren konijnen is
2. er geen konijnen sterven
3. konijnen zich vanaf 2 maanden voortplanten
4. vervolgens uit elk paar elke maand een nieuw paar geboren wordt

Noteer met  $f_n$  het aantal paren konijnen na  $n$  maanden. Dan is

$$f_0 = 0$$

$$f_1 = 1$$

$$f_n = f_{n-1} + f_{n-2} \quad \text{voor } n \geq 2$$

**Programma****Java-methode die  $f_n$  uitrekent**

```
int f(int n)
{ if (n <= 1) return n;
  return f(n-1) + f(n-2);
}
```

Dit programma is heel inefficiënt: het aantal aanroepen van  $f$  groeit exponentieel. (Voor het uitrekenen van elke waarde zijn twee nieuwe waarden nodig. De recurrente betrekking die het aantal aanroepen van  $f$  bepaalt, is afgezien van de startwaarden dezelfde als die voor  $f_n$ .)

**Beter programma****Java-methode die  $f_n$  efficiënter uitrekent**

```
int f(int n)
{ int f0 = 0;
  int f1 = 1;
  for (int k=0; k<n; k++)
  { //f0 = f(k), f1 = f(k+1)
    int f2 = f1 + f0;
    f0 = f1;
    f1 = f2;
  }
  return f0;
}
```

Uitvoer: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

Quotiënt van opeenvolgende termen: 1.00, 2.00, 1.50, 1.67, 1.60, 1.63, 1.62, 1.62, 1.62, ... Dit suggereert de aanwezigheid van een overheersende term  $1.62^n$ .

**Probeeroplossing**

Zoek naar oplossingen van de recurrentie  $f_n = f_{n-1} + f_{n-2}$  die van de vorm  $f_n = x^n$  zijn, waar  $x \neq 0$ . Er geldt

$$\begin{aligned}
 & f_n = f_{n-1} + f_{n-2} \\
 \Leftrightarrow & \{ \text{probeer } f_n = x^n \text{ voor alle } n \} \\
 & x^n = x^{n-1} + x^{n-2} \\
 \Leftrightarrow & \{ \text{als } x \neq 0 \} \\
 & x^2 = x + 1 \\
 \Leftrightarrow & \{ \text{rekenen} \} \\
 & x^2 - x - 1 = 0 \\
 \Leftrightarrow & \{ \text{vierkantsvergelijking} \} \\
 & x = (1 \pm \sqrt{5})/2
 \end{aligned}$$

**Beginwaarden**

Zij  $\phi = (1 + \sqrt{5})/2$  en  $\hat{\phi} = (1 - \sqrt{5})/2$ . Dan zijn  $f_n = \phi^n$  en  $f_n = \hat{\phi}^n$  oplossingen van de recurrentie  $f_n = f_{n-1} + f_{n-2}$ . Dat geldt dan ook voor de lineaire combinatie

$$f_n = C \cdot \phi^n + D \cdot \hat{\phi}^n$$

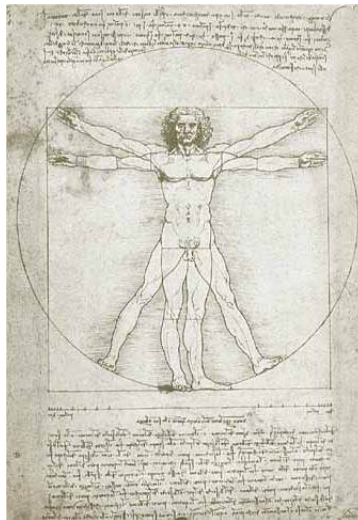
We zoeken nu C en D zodanig dat aan de startcondities is voldaan.

Substitutie van  $f_0 = 0$  geeft  $C + D = 0$  dus  $D = -C$ . En ad  $f_1$ :

$$\begin{aligned} f_1 &= \{ \text{probeer } f_n = C \cdot \phi^n + D \cdot \hat{\phi}^n \} \\ &= C \cdot \phi + D \cdot \hat{\phi} \\ &= \{ D = -C \} \\ &= C \cdot (\phi - \hat{\phi}) \\ &= \{ \phi = (1 + \sqrt{5})/2 \text{ en } \hat{\phi} = (1 - \sqrt{5})/2 \} \\ &= C \cdot \sqrt{5} \end{aligned}$$

dus  $f_1 = 1$  geeft  $C = 1/\sqrt{5}$ .

**Expliciete formule**



De Fibonaccigetallen  $f_n$  worden gegeven door

$$f_n = \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}} \text{ voor } n \geq 0$$

waar  $\phi = (1 + \sqrt{5})/2$  en  $\hat{\phi} = (1 - \sqrt{5})/2$ .

Het getal  $\phi = 1,61803...$  heet de Gulden Snede. De letter  $\phi$  verwijst naar Phidias, beeldhouwer van de Akropolis.

**Mathematica**

Invoer:

```
RSolve[{f[n] == f[n - 1] + f[n - 2], f[0] == 0, f[1] == 1}, f[n], n]
```

Uitvoer:

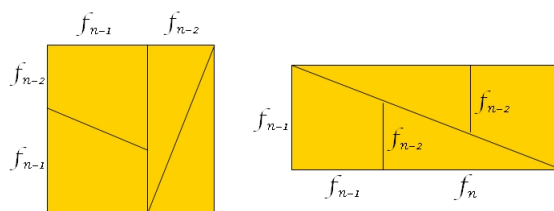
$$\left\{ \left\{ f(n) \rightarrow -\frac{\left(\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^n - \left(\frac{1}{2} + \frac{\sqrt{5}}{2}\right)^n}{\sqrt{5}} \right\} \right\}$$

**Eigenschappen van Fibonaccigetallen**

Jean-Dominique Cassini, 1680:

$$f_{n+1}f_{n-1} - f_n^2 = (-1)^n \text{ voor } n > 0$$

Puzzel (Lewis Carroll): neem  $f_n \times f_n$  schaakbord en verdeel het als volgt in vier stukken:



Je houdt dan 1 vierkantje over of komt er 1 tekort (bijv.  $8 \cdot 8 = 5 \cdot 13 - 1$ ).

**2.2 Euclides**

**Algoritme van Euclides**

Nu laten we een toepassing van Fibonaccigetallen in de informatica zien.

De grootste gemene deler van getallen  $a$  en  $b$  is het grootste positieve getal  $x$  zodanig dat zowel  $a$  als  $b$  zonder rest door  $x$  deelbaar zijn.

Eigenschappen:

$$\begin{aligned} \gcd(a, 0) &= a \\ \gcd(a, b) &= \gcd(b, a \bmod b) \end{aligned}$$

**Java-programma voor berekening van  $\gcd(a, b)$**

```
int gcd(int a, int b)
{ //pre a >= b
  while (b!=0)
  { int x=b;
    b=a%b;
    a=x;
  }
  return a;
}
```

**Complexiteit van Euclides' algoritme**

Nummer de achtereenvolgende waarden van  $b$  vanaf het laatste, dus  $b_0 = 0$  en  $b_1 \geq 1$  (anders was de herhaling al eerder gestopt). Verder steeds

$$b_i = b_{i+2} \bmod b_{i+1}$$

dus

$$b_{i+2} \geq b_i + b_{i+1}$$

Vergelijking met de recurrente betrekking voor de Fibonaccigetallen geeft

$$b_i \geq f_i$$

Als de startwaarde  $a$  aanleiding geeft tot  $n$  iteraties, geldt dus  $a \geq f_n \approx \phi^n / \sqrt{5}$ , dus

$$n \leq \phi \log(\sqrt{5}a) \approx 1.67 + 1.44 \cdot \log a$$

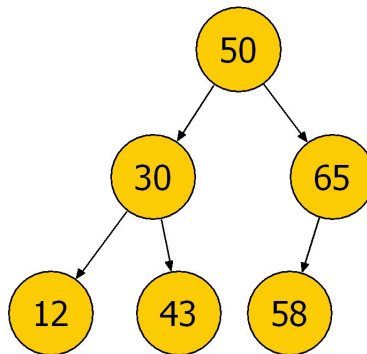
**2.3 AVL****AVL-bomen**

Een binaire boom bestaat uit een wortel en twee subbomen die leeg zijn of zelf weer een binaire boom vormen.

Binaire bomen zijn geschikt als datastructuur, in het bijzonder als we links van de wortel alleen elementen kleiner dan dat in de wortel opnemen en rechts alleen groter. We spreken dan van een zoekboom.

De efficiëntie van het zoeken in een zoekboom hangt af van de diepte, dat is het langste pad.

Adelson-Velskii en Landis, 1962: een AVL-boom is een zoekboom waarin de diepte van linker- en rechtersubbomen steeds niet meer dan 1 verschillen.

**Maximale diepte van een AVL-boom**

Zij  $M_i$  het minimale aantal elementen in een AVL-boom van diepte  $i$ . Dan is  $M_1 = 1$ ,  $M_2 = 2$ .

Beschouw het geval  $i \geq 2$ . Een van de subbomen van de wortel heeft dan diepte  $i - 1$ , de andere diepte ten minste  $i - 2$ . Als we deze vervangen door minimale AVL-bomen van diepte  $i - 1$  respectievelijk  $i - 2$ , zal het aantal elementen niet toenemen. Dus

$$M_i = M_{i-1} + M_{i-2} + 1$$

Dit lijkt op de recurrente betrekking voor Fibonaccigetallen, en we kunnen het op dezelfde manier aanpakken. Maar we kunnen ook ons oude resultaat hergebruiken.

Definieer  $L_i = M_i + 1$ . We leiden een recurrente betrekking voor  $L_i$  af.

### Coördinatentransformatie

$$\begin{aligned} L_i & \\ &= \quad \{\text{definitie}\} \\ & M_i + 1 \\ &= \quad \{\text{recurrente betrekking}\} \\ & (M_{i-1} + M_{i-2} + 1) + 1 \\ &= \quad \{\text{rekenen}\} \\ & (M_{i-1} + 1) + (M_{i-2} + 1) \\ &= \quad \{\text{definitie}\} \\ & L_{i-1} + L_{i-2} \end{aligned}$$

Verder  $L_1 = 2 = f_3$  en  $L_2 = 3 = f_4$ , dus

$$M_i \approx L_i = f_{i+2} \approx \frac{\phi^2}{\sqrt{5}} \phi^i$$

Dus als  $n$  elementen zijn opgeslagen in een AVL-boom van diepte  $k$ , geldt  $n \geq \frac{\phi^2}{\sqrt{5}} \phi^k$  ofwel

$$k \leq \phi \log(n \cdot \frac{\sqrt{5}}{\phi^2}) \approx 1.44 \cdot \log n - 0.33$$

## 2.4 Mergesort

### Mergesort

Sorteren van een lijst  $a$  op recursieve wijze: sorteert twee helften afzonderlijk en voeg ze samen.

### Mergesort

```
void mergesort(int[] a, int l, int r)
{ int m = (l + r) / 2;
  if (l < m)
  { mergesort(a, l, m);
    int[] b = new int[m-l]; System.arraycopy(a, l, b, 0, m-l);
    mergesort(a, m, r);
    int[] c = new int[r-m]; System.arraycopy(a, m, c, 0, r-m);
```

```

int i = 0; int j = 0; int k = 1;
while (i < m-1 && j < r-m)
  if (b[i] < c[j]) a[k++] = b[i++]; else a[k++] = c[j++];
  System.arraycopy(b, i, a, k, m-1-i);
  System.arraycopy(c, j, a, k+m-1-i, r-m-j);
}
}

```

### Recurrente betrekking

We introduceren  $M_n$  als een bovengrens voor het aantal vergelijkingen dat nodig is om een lijst van  $n$  elementen te sorteren met Mergesort. Uit de programmeertekst blijkt dat we kunnen kiezen  $M_1 = 0$ , en voor  $k \geq 1$

$$M_{2k} = 2M_k + 2k - 1$$

$$M_{2k+1} = M_k + M_{k+1} + 2k$$

Noteer met  $L_n$  het kleinste getal  $i$  waarvoor  $2^i \geq n$ . (Dan  $L_n \approx \lceil \log_2 n \rceil$ .) We zullen bewijzen dat

$$M_n = nL_n - 2^{L_n} + 1$$

voor alle  $n$ , met inductie. Basis: de bewering geldt voor  $n = 1$ . Stap: zij  $n > 1$  en veronderstel dat de bewering geldt voor alle voorgangers van  $n$ . Zij  $n = 2k$  of  $n = 2k + 1$ ; we zullen de bewering in het bijzonder voor  $k$  en  $k + 1$  gebruiken.

Als  $n = 2k$ , is zeker  $L_n = L_k + 1$ . Als  $n = 2k + 1$ , onderscheiden we twee aparte gevallen:

1.  $k$  is geen macht van 2; dan  $L_n = L_{k+1} + 1 = L_k + 1$
2.  $k$  is een macht van 2; dan  $L_n = L_{k+1} + 1 = L_k + 2$

### Complexiteit van Mergesort: eerste geval

Zij  $n = 2k$ . Dan

$$\begin{aligned}
& M_n \\
= & \{ n \text{ even; recurrente betrekking} \} \\
& 2M_k + 2k - 1 \\
= & \{ \text{inductiehypothese voor } k \} \\
& 2(kL_k - 2^{L_k} + 1) + 2k - 1 \\
= & \{ n = 2k, \text{ dus } L_k = L_n - 1 \} \\
& 2(k(L_n - 1) - 2^{L_n - 1} + 1) + 2k - 1 \\
= & \{ \text{rekenen} \} \\
& 2kL_n - 2^{L_n} + 1 \\
= & \{ 2k = n \} \\
& nL_n - 2^{L_n} + 1
\end{aligned}$$

**Complexiteit van Mergesort: tweede geval**

Zij  $n = 2k + 1$ ,  $k$  geen macht van 2. Dan

$$\begin{aligned}
 & M_n \\
 = & \quad \{ n \text{ oneven; recurrente betrekking} \} \\
 & M_k + M_{k+1} + 2k \\
 = & \quad \{ \text{inductiehypothese voor } k \text{ en } k + 1 \} \\
 & (kL_k - 2^{L_k} + 1) + ((k + 1)L_{k+1} - 2^{L_{k+1}} + 1) + 2k \\
 = & \quad \{ k \text{ geen macht van } 2, \text{ dus } L_k = L_{k+1} = L_n - 1 \} \\
 & (k(L_n - 1) - 2^{L_n - 1} + 1) + ((k + 1)(L_n - 1) - 2^{L_n - 1} + 1) + 2k \\
 = & \quad \{ \text{rekenen} \} \\
 & (2k + 1)L_n - 2^{L_n} + 1 \\
 = & \quad \{ 2k + 1 = n \} \\
 & nL_n - 2^{L_n} + 1
 \end{aligned}$$

**Complexiteit van Mergesort: derde geval**

Zij  $n = 2k + 1$ ,  $k$  een macht van 2. Dan

$$\begin{aligned}
 & M_n \\
 = & \quad \{ n \text{ oneven; recurrente betrekking} \} \\
 & M_k + M_{k+1} + 2k \\
 = & \quad \{ \text{inductiehypothese voor } k \text{ en } k + 1 \} \\
 & (kL_k - 2^{L_k} + 1) + ((k + 1)L_{k+1} - 2^{L_{k+1}} + 1) + 2k \\
 = & \quad \{ k \text{ een macht van } 2, \text{ dus } L_k = L_n - 2, L_{k+1} = L_n - 1 \} \\
 & (k(L_n - 2) - 2^{L_n - 2} + 1) + ((k + 1)(L_n - 1) - 2^{L_n - 1} + 1) + 2k \\
 = & \quad \{ \text{rekenen} \} \\
 & (2k + 1)L_n - 3 \cdot 2^{L_n - 2} - k + 1 \\
 = & \quad \{ \text{rekenen} \} \\
 & (2k + 1)L_n - 2^{L_n} + 2^{L_n - 2} - k + 1 \\
 = & \quad \{ k \text{ een macht van } 2, \text{ dus } k = 2^{L_k} = 2^{L_n - 2} \} \\
 & (2k + 1)L_n - 2^{L_n} + 1 \\
 = & \quad \{ 2k + 1 = n \} \\
 & nL_n - 2^{L_n} + 1
 \end{aligned}$$

**Complexiteit van Mergesort: conclusie**

Sorteren van een rij van  $n$  getallen met Mergesort kost

$$nL_n - 2^{L_n} + 1 \approx n \cdot 2 \log n$$

vergelijkingen. Voorbeeld: voor  $n = 1000$  is  $L_n = 10$ , dus er zijn  $10000 - 1024 + 1 = 8977$  vergelijkingen nodig.

Dit resultaat is niet essentieel te verbeteren: beschouw sorteren als het zoeken van de unieke stijgende permutatie. Elke vergelijking halveert de zoekruimte van mogelijke permutaties. In totaal zijn er  $n!$  permutaties, dus er zijn

$$L_n! \approx n \cdot 2 \log n$$

vergelijkingen nodig.

## 2.5 Algemene oplossing

### Homogene lineaire betrekkingen van orde 2: reële oplossingen

Beschouw de recurrente betrekking

$$t_n = At_{n-1} + Bt_{n-2} \quad \text{voor } n \geq 2$$

Drie gevallen:

1. De vergelijking  $x^2 - Ax - B = 0$  heeft twee verschillende reële wortels  $p$  en  $q$ . Dan is de algemene oplossing

$$t_n = Cp^n + Dq^n$$

De coëfficiënten  $C$  en  $D$  worden bepaald door  $t_0$  en  $t_1$  (zie Fibonacci).

2. De vergelijking  $x^2 - Ax - B = 0$  heeft een enkele reële wortel  $p$ . Dan is de algemene oplossing

$$t_n = Cp^n + Dnp^n$$

Wederom worden de coëfficiënten  $C$  en  $D$  bepaald door  $t_0$  en  $t_1$ .

### Homogene lineaire betrekkingen van orde 2: complexe oplossingen

3. De vergelijking  $x^2 - Ax - B = 0$  heeft geen reële wortels. Dan is de algemene oplossing van de vorm

$$t_n = Cr^n \cos(n\phi) + Dr^n \sin(n\phi)$$

Voor het bepalen van  $r$  en  $\phi$  hebben we complexe getallen nodig: de complexe wortels van de vergelijking zijn  $r \cos \phi \pm ir \sin \phi$ . Vervolgens worden de coëfficiënten  $C$  en  $D$  weer bepaald door  $t_0$  en  $t_1$ .

### Inhomogene lineaire betrekkingen

Beschouw de recurrente betrekking

$$t_n = A_1 t_{n-1} + A_2 t_{n-2} + \dots + A_k t_{n-k} + f(n) \quad \text{voor } n \geq k$$

met gegeven startwaarden  $t_0, \dots, t_k$ . De oplossing is als volgt te vinden:

1. Vind *een* particuliere oplossing  $p_n$  (d.w.z. een rij die aan de recurrente betrekking maar misschien niet aan de startwaarden voldoet)
2. Bepaal de *algemene* oplossing  $a_n$  van het homogene probleem (dus  $f(n)$  door 0 vervangen)
3. De algemene oplossing van het inhomogene probleem is de som  $p_n + a_n$
4. Bepaal de waarden van de constanten die in deze algemene oplossing voorkomen uit de gegeven startwaarden

**Inhomogene lineaire betrekkingen:voorbeeld**

Beschouw de recurrente betrekking

$$t_n = 2t_{n-2} + 3n$$

met  $t_0 = 4$ ,  $t_1 = 2$ . Particuliere oplossing: Probeer  $p_n$  van dezelfde gedaante als de dwangterm:  $p_n = an + b$ . Substitutie in de recurrente betrekking geeft

$$\begin{aligned} p_n &= 2p_{n-2} + 3n \\ \Leftrightarrow \{ p_n = an + b \} \\ an + b &= 2(a(n-2) + b) + 3n \\ \Leftrightarrow \{ \text{rekenen} \} \\ (-a - 3)n + (4a - b) &= 0 \\ \Leftrightarrow \{ \text{coëfficiënten nul stellen} \} \\ -a - 3 = 0 \wedge 4a - b &= 0 \\ \Leftrightarrow \{ \text{rekenen} \} \\ a = -3 \wedge b &= -12 \end{aligned}$$

dus een particuliere oplossing is  $p_n = -3n - 12$ .

**Inhomogene lineaire betrekkingen:voorbeeld**

Algemene oplossing van de homogene betrekking: de homogene vergelijking is

$$t_n = 2t_{n-2}$$

Beschouw de vergelijking  $x^2 - 2 = 0$ ; deze heeft als oplossing  $x = \pm\sqrt{2}$ . De algemene oplossing van de homogene betrekking is daarom

$$t_n = (C + D(-1)^n)(\sqrt{2})^n$$

De algemene oplossing van het inhomogene probleem is dus

$$t_n = (C + D(-1)^n)(\sqrt{2})^n - 3n - 12$$

Substitutie van  $t_0 = 4$  en  $t_1 = 2$  geeft

$$C + D - 12 = 4 \wedge (C - D)\sqrt{2} - 15 = 2$$

ofwel

$$C = 8 + \frac{17}{4}\sqrt{2} \wedge D = 8 - \frac{17}{4}\sqrt{2}$$

**Mathematica**

Invoer:

```
RSolve[{t[n] == 2t[n - 2] + 3n, t[0] == 4, t[1] == 2}, t[n], n]
```

Uitvoer:

$$\left\{ \left\{ t(n) \rightarrow -\frac{3(-1)^{2n}n + 3(-1)^{2n}\sqrt{2}n + 15\sqrt{2}n + 21n - 7(-1)^n 2^{\frac{n}{2} + \frac{3}{2}} - 412^{\frac{n}{2} + \frac{3}{2}} - 13(-1)^n 2^{n/2} - 1152^{n/2} + 3(-1)^{2n} + 6(-1)^{2n}\sqrt{2} + 66\sqrt{2} + 93}{(-2 + \sqrt{2})^2 (1 + \sqrt{2}) (2 + \sqrt{2}) (3 + 2\sqrt{2})} \right\} \right\}$$

Invoer:

FullSimplify[%, n ∈ Integers]

Uitvoer:

$$\left\{ \left\{ t(n) \rightarrow 2^{\frac{n}{2}-2} \left( 32 + 17\sqrt{2} + (-1)^n \left( 32 - 17\sqrt{2} \right) \right) - 3(n + 4) \right\} \right\}$$

### 3 Sommatie

#### 3.1 De sigma-notatie

##### De sigma-notatie

De notatie

$$1 + 2 + \dots + 2^{n-1}$$

is ambigu: bedoelen we

$$1 + 2 + 3 + 4 + 5 + \dots + 2^{n-1} - 1 + 2^{n-1}$$

of

$$1 + 2 + 4 + 8 + 16 + \dots + 2^{n-2} + 2^{n-1} \quad ?$$

En heeft dit ook betekenis als  $n = 1$ , of als  $n = 0$ ? Om dubbelzinnigheid uit te sluiten, introduceerde Joseph Fourier in 1820 de notatie

$$\sum_{k=1}^n a_k$$

Hierin heet  $a_k$  de term, 1 en  $n$  de onder- en bovengrens, en  $k$  de gebonden variabele. De naam  $k$  moet in de context nog geen betekenis hebben, maar is verder irrelevant.

##### De Iverson-conventie

Met de sigma-notatie kunnen we goed onderscheid maken tussen

$$\sum_{k=1}^{2^{n-1}} k$$

en

$$\sum_{j=0}^{n-1} 2^j$$

Maar soms willen we ook sommeren over een niet-aaneengesloten gebied. In de literatuur zie je vaak iets als

$$\sum_{p^2+q^2 \leq n} \frac{1}{p+q}, \quad \sum_{f(n)=0} n$$

Nadelen: veel en belangrijke informatie moet in het onderschrift worden geperst, en het is niet altijd duidelijk wat de gebonden variabele is. Liever schrijven we

$$\sum_{p=1}^n \frac{[p^2+q^2 \leq n]}{p+q}, \quad \sum_n [f(n)=0]n$$

### De Iverson-conventie

Kenneth Iverson, 1962: Voor een conditie ('boolean expressie')  $p$  noteren we

$$[p] = \begin{cases} 1 & \text{als } p \\ 0 & \text{als niet } p \end{cases}$$

Daarbij hanteren we de afspraak dat  $[p_k]a_k = 0$  als  $p_k$  onwaar is, zelfs als  $a_k$  dan ongedefinieerd is. Voorbeeld:

$$\sum_{i=0}^{10} \frac{[i \neq 5]}{i-5} = 0$$

De notatie is erg handig voor transformatie van de gebonden variabele: de transformatie  $k \leftarrow 99 - k$  geeft

$$\sum_k [0 \leq k < n]a_k = \sum_k [0 \leq 99 - k < n]a_{99-k} = \sum_k [99 - n < k \leq 99]a_{99-k}$$

## 3.2 Sommatiefactor

### Recurrente betrekkingen met niet-constante coëfficiënten

Beschouw een recurrente betrekking van de vorm

$$a_n T_n = b_n T_{n-1} + c_n$$

Kies nu  $s_n$  zó dat

$$s_n b_n = a_{n-1} s_{n-1}$$

Met  $S_n = s_n a_n T_n$  is de recurrente betrekking dan equivalent met

$$S_n = S_{n-1} + s_n c_n$$

dus de algemene oplossing is

$$S_n = S_0 + \sum_{k=1}^n s_k c_k$$

ofwel

$$T_n = \frac{1}{s_n a_n} \left( s_1 b_1 T_0 + \sum_{k=1}^n s_k c_k \right)$$

**Sommatiefactor**

$$a_n T_n = b_n T_{n-1} + c_n$$

heeft dus de algemene oplossing

$$T_n = \frac{1}{s_n a_n} \left( s_1 b_1 T_0 + \sum_{k=1}^n s_k c_k \right)$$

waarin

$$s_n b_n = a_{n-1} s_{n-1}$$

dus

$$s_n = \frac{a_{n-1} s_{n-1}}{b_n} = \frac{a_{n-1} a_{n-2} s_{n-2}}{b_n b_{n-1}} = \dots = \frac{a_{n-1} a_{n-2} \dots a_1}{b_n b_{n-1} \dots b_2}$$

Deze  $s_n$  heet de *sommatiefactor*.

**3.3 Quicksort****Quicksort****Quicksort**

```
void quicksort(int[] a, int l, int r)
{ if (l < r-1)
  { int t, v, i, j;
    v = a[r-1]; i = l-1; j = r-1;
    do
    { do i++; while (a[i] < v);
      do j--; while (a[j] > v);
      t = a[i]; a[i] = a[j]; a[j] = t;
    }
    while (i < j);
    a[j] = a[i]; a[i] = a[r-1]; a[r-1] = t;
    quicksort(a, l, i);
    quicksort(a, i+1, r);
  }
}
```

**Quicksort**

Idee achter Quicksort: kies een waarde  $v$  in de lijst, en herschik de waarden zo dat links van  $v$  alleen termen  $\leq v$  en rechts alleen termen  $\geq v$  staan. Dan zijn verder alleen nog permutaties binnen het linker- en rechterstuk nodig! Pas dan `quicksort` opnieuw toe op die twee stukken.

Hoeveel vergelijkingen heeft Quicksort nodig om  $n$  verschillende elementen te sorteren? Noem  $C_n$  het aantal vergelijkingen dat daarvoor *gemiddeld* nodig is. Dan is  $C_0 = 0$  en

$$C_n = n + 1 + \frac{1}{n} \sum_{j=1}^n (C_{j-1} + C_{n-j})$$

De term met index  $j$  correspondeert met het geval dat er  $j - 1$  elementen kleiner dan  $v$  en  $n - j$  elementen groter dan  $v$  in de lijst voorkomen. Alle waarden  $j$  met  $1 \leq j \leq n$  zijn even waarschijnlijk.

### Complexiteit van Quicksort

$$\begin{aligned} & \sum_{j=1}^n (C_{j-1} + C_{n-j}) \\ = & \quad \{\text{termsplitsing}\} \\ & \sum_{j=1}^n C_{j-1} + \sum_{j=1}^n C_{n-j} \\ = & \quad \{\text{dummytransformatie } j \leftarrow n - j + 1\} \\ & \sum_{j=1}^n C_{j-1} + \sum_{j=1}^n C_{j-1} \\ = & \quad \{\text{beide sommen zijn identiek}\} \\ & 2 \sum_{j=1}^n C_{j-1} \end{aligned}$$

De gebruikte rekenregels moeten we nog nader onderzoeken...

Dit geeft de vereenvoudigde recurrente betrekking:  $C_0 = 0$  en

$$C_n = n + 1 + \frac{2}{n} \sum_{j=1}^n C_{j-1} \quad \text{voor } n > 0$$

### Complexiteit van Quicksort

$$\begin{aligned} & C_n = n + 1 + \frac{2}{n} \sum_{j=1}^n C_{j-1} \quad \text{voor } n > 0 \\ \Leftrightarrow & \quad \{\text{vermenigvuldig beide leden met } n\} \\ & nC_n = n(n + 1) + 2 \sum_{j=1}^n C_{j-1} \quad \text{voor } n > 0 \\ \Leftrightarrow & \quad \{\text{dummytransformatie } n \leftarrow n - 1\} \\ & nC_n = n(n + 1) + 2 \sum_{j=1}^n C_{j-1} \quad \text{voor } n > 0 \\ & \wedge (n - 1)C_{n-1} = (n - 1)n + 2 \sum_{j=1}^{n-1} C_{j-1} \quad \text{voor } n - 1 > 0 \\ \Rightarrow & \quad \{\text{trek tweede vergelijking van eerste af}\} \\ & nC_n - (n - 1)C_{n-1} = 2n + 2C_{n-1} \quad \text{voor } n > 1 \\ \Leftrightarrow & \quad \{\text{breng alle termen met } C_{n-1} \text{ naar rechts}\} \\ & nC_n = (n + 1)C_{n-1} + 2n \quad \text{voor } n > 1 \\ \Leftrightarrow & \quad \{\text{formule geldt ook voor } n = 1 \text{ omdat } C_0 = 0 \text{ en } C_1 = 2\} \\ & nC_n = (n + 1)C_{n-1} + 2n \quad \text{voor } n > 0 \end{aligned}$$

Deze recurrente betrekking laat een sommatiefactor toe:

$$s_n = \frac{(n - 1) \cdot (n - 2) \cdot \dots \cdot 1}{(n + 1) \cdot n \cdot \dots \cdot 3} = \frac{2}{n(n + 1)}$$

### Harmonische getallen

De algemene oplossing van de recurrente betrekking voor de (gemiddelde) complexiteit van Quicksort is

$$C_n = 2(n+1) \sum_{k=1}^n \frac{1}{k+1}$$

Vaak voorkomende grootheid: het  $n$ -de harmonische getal  $H_n$  is gedefinieerd als  $H_n = \sum_{k=1}^n \frac{1}{k}$ . We kunnen  $C_n$  uitdrukken in  $H_n$ : er geldt  $C_n = 2(n+1)H_n - 2n$ . Aan het eind van dit college zullen we zien dat  $H_n \geq \ln(n+1)$ ; voor grote  $n$  is ruwweg  $H_n \approx \ln n$ .

### Harmonische getallen

$$\begin{aligned} & C_n \\ = & \quad \{ \text{algemene oplossing} \} \\ & 2(n+1) \sum_{k=1}^n \frac{1}{k+1} \\ = & \quad \{ \text{dummytransformatie } k \leftarrow k-1 \} \\ & 2(n+1) \sum_{k=2}^{n+1} \frac{1}{k} \\ = & \quad \{ \text{voeg toe } k=1, \text{ gebruik } n \geq 0 \} \\ & 2(n+1) \sum_{k=1}^{n+1} \frac{1}{k} - 2(n+1) \\ = & \quad \{ \text{splits af } k=n+1, \text{ gebruik } n \geq 0 \} \\ & 2(n+1) \sum_{k=1}^n \frac{1}{k} + 2 - 2(n+1) \\ = & \quad \{ \text{definitie } H_n; \text{ rekenen} \} \\ & 2(n+1)H_n - 2n \end{aligned}$$

## 3.4 Rekenregels

### Rekenregels

Distributie van vermenigvuldiging over optelling:

$$c \sum_k a_k = \sum_k ca_k$$

Termsplitsing:

$$\sum_k (a_k + b_k) = \sum_k a_k + \sum_k b_k$$

Domeinsplitsing:

$$\sum_{k \in A \cup B} a_k = \sum_{k \in A} a_k + \sum_{k \in B} a_k \quad \text{als } A \cap B = \emptyset$$

Leeg domein:

$$\sum_{k \in \emptyset} a_k = 0$$

## Rekenregels

Eenpuntsregel:

$$\sum_{k \in \{p\}} a_k = a_p$$

Constante term:

$$\sum_{k \in A} c = c \cdot \#A$$

Monotonie:

$$\sum_k a_k \leq \sum_k b_k \text{ als } a_k \leq b_k \text{ voor alle } k$$

Dummytransformatie  $k \leftarrow p(k)$ :

$$\sum_{k \in A} a_k = \sum_{p(k) \in A} a_{p(k)} \text{ als } p \text{ permutatie van } \mathbb{Z}$$

(Een permutatie van  $Z$  neemt elke gehele waarde precies eenmaal aan. Voorbeelden:  $p(k) = c + k$ ,  $p(k) = c - k$ .)

## Rekenkundige rijen

Formalisering van argument van Gauss uit het eerste college:

$$\begin{aligned} & \sum_{k=0}^n (a + bk) \\ = & \quad \{\text{verdubbeling}\} \\ & \frac{1}{2} (\sum_{k=0}^n (a + bk) + \sum_{k=0}^n (a + bk)) \\ = & \quad \{\text{dummytransformatie } k \leftarrow n - k\} \\ & \frac{1}{2} (\sum_{k=0}^n (a + bk) + \sum_{k=0}^n (a + b(n - k))) \\ = & \quad \{\text{termsplitsing}\} \\ & \frac{1}{2} (\sum_{k=0}^n (a + bk + a + b(n - k))) \\ = & \quad \{\text{rekenen}\} \\ & \frac{1}{2} (\sum_{k=0}^n (2a + bn)) \\ = & \quad \{\text{constante term}\} \\ & \frac{1}{2} (n + 1)(2a + bn) \end{aligned}$$

## Afsplitsen van een term

Afgeleide regel:

$$\begin{aligned} & \sum_{k=p}^q a_k \\ = & \quad \{\text{domeinsplitsing, Iverson}\} \\ & \sum_k [p \leq k \leq q \wedge k \neq q] a_k + \sum_k [p \leq k \leq q \wedge k = q] a_k \\ = & \quad \{\text{vereenvoudiging domeinen}\} \\ & \sum_k [p \leq k \leq q - 1] a_k + \sum_k [p \leq q \wedge k = q] a_k \\ = & \quad \{\text{mits } p \leq q\} \\ & \sum_{k=p}^{q-1} a_k + \sum_{k=q}^q a_k \\ = & \quad \{\text{eenpuntsregel}\} \\ & \sum_{k=p}^{q-1} a_k + a_q \end{aligned}$$

dus

$$\sum_{k=p}^q a_k = \sum_{k=p}^{q-1} a_k + a_q \text{ als } p \leq q$$

De voorwaarde is nodig!

### Meetkundige rijen

Voor  $S_n = \sum_{k=0}^n ax^k$  is

$$\begin{aligned} S_{n+1} &= \{ \text{definitie} \} \\ &= \sum_{k=0}^{n+1} ax^k \\ &= \{ \text{splits af } k=0, \text{ gebruik } 0 \leq n+1 \} \\ &= a + \sum_{k=1}^{n+1} ax^k \\ &= \{ \text{dummytransformatie } k \leftarrow k+1 \} \\ &= a + \sum_{k=0}^n ax^{k+1} \\ &= \{ \text{distributie van vermenigvuldiging over sommatie} \} \\ &= a + x \sum_{k=0}^n ax^k \\ &= \{ \text{definitie} \} \\ &= a + xS_n \end{aligned}$$

### Meetkundige rijen

We hebben afgeleid  $S_{n+1} = a + xS_n$ . Maar ook

$$\begin{aligned} S_{n+1} &= \{ \text{definitie} \} \\ &= \sum_{k=0}^{n+1} ax^k \\ &= \{ \text{splits af } k=n+1, \text{ gebruik } 0 \leq n+1 \} \\ &= \sum_{k=0}^n ax^k + ax^{n+1} \\ &= \{ \text{definitie} \} \\ &= S_n + ax^{n+1} \end{aligned}$$

dus  $S_n + ax^{n+1} = a + xS_n$ , waaruit volgt

$$S_n = a \frac{1 - x^{n+1}}{1 - x} \text{ als } x \neq 1$$

### Dubbelsommen

Verwisselen van sommatie:

$$\sum_j \sum_k [P(j, k)] a_{j,k} = \sum_k \sum_j [P(j, k)] a_{j,k}$$

Simpel geval: als de domeinen voor  $j$  en  $k$  onafhankelijk zijn. Dan

$$\sum_{j \in J} \sum_{k \in K} a_{j,k} = \sum_{k \in K} \sum_{j \in J} a_{j,k}$$

Interessant geval: als het domein voor  $k$  afhangt van  $j$ . Bijvoorbeeld

$$\sum_{j=1}^n \sum_{k=j}^n a_{j,k} = \sum_{k=1}^n \sum_{j=1}^k a_{j,k}$$

### Dubbelsommen

$$\begin{aligned} & \sum_{j=1}^n \sum_{k=j}^n a_{j,k} \\ = & \quad \{\text{Iverson}\} \\ & \sum_j [1 \leq j \leq n] \sum_k [j \leq k \leq n] a_{j,k} \\ = & \quad \{\text{distributie}\} \\ & \sum_j \sum_k [1 \leq j \leq n] [j \leq k \leq n] a_{j,k} \\ = & \quad \{ [P][Q] = [P \wedge Q]; \text{transitiviteit van } \leq \} \\ & \sum_j \sum_k [1 \leq j \leq k \leq n] a_{j,k} \\ = & \quad \{\text{verwisselen van sommatie}\} \\ & \sum_k \sum_j [1 \leq j \leq k \leq n] a_{j,k} \\ = & \quad \{ [P][Q] = [P \wedge Q]; \text{transitiviteit van } \leq \} \\ & \sum_k \sum_j [1 \leq k \leq n] [1 \leq j \leq k] a_{j,k} \\ = & \quad \{\text{distributie}\} \\ & \sum_k [1 \leq k \leq n] \sum_j [1 \leq j \leq k] a_{j,k} \\ = & \quad \{\text{Iverson}\} \\ & \sum_{k=1}^n \sum_{j=1}^k a_{j,k} \end{aligned}$$

### Ongelijkheid van Chebyshev

$$\begin{aligned} & \sum_{j=1}^n \sum_{k=j+1}^n (a_k - a_j)(b_k - b_j) \\ = & \quad \{\text{verdubbeling}\} \\ & \frac{1}{2} \left( \sum_{j=1}^n \sum_{k=j+1}^n (a_k - a_j)(b_k - b_j) + \sum_{j=1}^n \sum_{k=j+1}^n (a_k - a_j)(b_k - b_j) \right) \\ = & \quad \{\text{dummytransformatie } j, k \leftarrow k, j \} \\ & \frac{1}{2} \left( \sum_{j=1}^n \sum_{k=j+1}^n (a_k - a_j)(b_k - b_j) + \sum_{k=1}^n \sum_{j=k+1}^n (a_j - a_k)(b_j - b_k) \right) \\ = & \quad \{\text{verwisselen van sommatie}\} \\ & \frac{1}{2} \left( \sum_{j=1}^n \sum_{k=j+1}^n (a_k - a_j)(b_k - b_j) + \sum_{j=1}^n \sum_{k=1}^{j-1} (a_j - a_k)(b_j - b_k) \right) \\ = & \quad \{\text{domeinsplitsing; splits af } k = j \} \\ & \frac{1}{2} \sum_{j=1}^n \sum_{k=1}^n (a_k - a_j)(b_k - b_j) \\ = & \quad \{\text{termsplitsing; dummytransformatie } j, k \leftarrow k, j \} \\ & \sum_{j=1}^n \sum_{k=1}^n a_k b_k - \sum_{j=1}^n \sum_{k=1}^n a_j b_k \\ = & \quad \{\text{constante term; distributie}\} \\ & n \sum_{k=1}^n a_k b_k - \left( \sum_{j=1}^n a_j \right) \left( \sum_{k=1}^n b_k \right) \end{aligned}$$

### Ongelijkheid van Chebyshev

Conclusie:

$$\left(\sum_{j=1}^n a_j\right)\left(\sum_{k=1}^n b_k\right) = n \sum_{k=1}^n a_k b_k - \sum_{j=1}^n \sum_{k=j+1}^n (a_k - a_j)(b_k - b_j)$$

dus

$$\left(\sum_{j=1}^n a_j\right)\left(\sum_{k=1}^n b_k\right) \leq n \sum_{k=1}^n a_k b_k$$

als  $a_1 \leq a_2 \leq \dots \leq a_n$  en  $b_1 \leq b_1 \leq \dots \leq b_n$ , en

$$\left(\sum_{j=1}^n a_j\right)\left(\sum_{k=1}^n b_k\right) \geq n \sum_{k=1}^n a_k b_k$$

als  $a_1 \leq a_2 \leq \dots \leq a_n$  en  $b_1 \geq b_1 \geq \dots \geq b_n$ .

### Sommen en integralen

Stel dat we  $\sum_{k=0}^n k^2$  willen berekenen. We kennen wel een integraal die erop lijkt, namelijk

$$\int_0^n x^2 dx = \frac{n^3}{3}$$

En we kunnen ook het verschil berekenen:

$$\begin{aligned} & \sum_{k=0}^n k^2 - \int_0^n x^2 dx \\ = & \quad \{\text{integratie is additief}\} \\ & \sum_{k=1}^n \left(k^2 - \int_{k-1}^k x^2 dx\right) \\ = & \quad \{\text{primitieve van } x^2 \text{ is } x^3/3\} \\ & \sum_{k=1}^n \left(k^2 - (k^3/3 - (k-1)^3/3)\right) \\ = & \quad \{\text{rekenen}\} \\ & \sum_{k=1}^n \left(k - \frac{1}{3}\right) \\ = & \quad \{\text{termsplitsing; constante term}\} \\ & \sum_{k=1}^n k - \frac{n}{3} \\ = & \quad \{\text{rekenkundige rij}\} \\ & \frac{n(n+1)}{2} - \frac{n}{3} \end{aligned}$$

### Sommen en integralen

Conclusie:

$$\begin{aligned} & \sum_{k=0}^n k^2 \\ = & \quad \{\text{vergelijk met integraal}\} \\ & \int_0^n x^2 dx + \sum_{k=0}^n k^2 - \int_0^n x^2 dx \\ = & \quad \{\text{voorgaande}\} \\ & \frac{n^3}{3} + \frac{n(n+1)}{2} - \frac{n}{3} \\ = & \quad \{\text{rekenen}\} \\ & \frac{2n^3 + 3n^2 + n}{6} \end{aligned}$$

### Sommen en integralen

Voor het harmonische getal  $H_n$  kunnen we als volgt een afschatting berekenen.

$$\begin{aligned}
 & \int_1^n \frac{dx}{x} \\
 = & \quad \{\text{domeinsplitsing}\} \\
 & \sum_{k=1}^{n-1} \int_k^{k+1} \frac{dx}{x} \\
 \leq & \quad \left\{ \frac{1}{x} \leq \frac{1}{k} \text{ voor } k \leq x \leq k+1 \right\} \\
 & \sum_{k=1}^{n-1} \int_k^{k+1} \frac{dx}{k} \\
 = & \quad \{\text{constante term}\} \\
 & \sum_{k=1}^{n-1} \frac{1}{k} \\
 = & \quad \{\text{splits af } k = n\} \\
 & \sum_{k=1}^n \frac{1}{k} - \frac{1}{n} \\
 = & \quad \{\text{per definitie}\} \\
 & H_n - \frac{1}{n}
 \end{aligned}$$

maar de beschouwde integraal is  $\ln n$ , dus  $H_n \geq \ln n + \frac{1}{n}$ .

### Sommen en integralen

Evenzo

$$\begin{aligned}
 & \sum_{k=1}^{n-1} \int_k^{k+1} \frac{dx}{x} \\
 \geq & \quad \left\{ \frac{1}{x} \geq \frac{1}{k+1} \text{ voor } k \leq x \leq k+1 \right\} \\
 & \sum_{k=1}^{n-1} \int_k^{k+1} \frac{dx}{k+1} \\
 = & \quad \{\text{constante term}\} \\
 & \sum_{k=1}^{n-1} \frac{1}{k+1} \\
 = & \quad \{\text{dummytransformatie } k \leftarrow k-1\} \\
 & \sum_{k=2}^n \frac{1}{k} \\
 = & \quad \{\text{splits af } k = 1\} \\
 & \sum_{k=1}^n \frac{1}{k} - 1 \\
 = & \quad \{\text{per definitie}\} \\
 & H_n - 1
 \end{aligned}$$

Conclusie:

$$\ln n + \frac{1}{n} \leq H_n \leq \ln n + 1$$

Voor grote  $n$  kunnen we dus zeggen dat  $H_n \approx \ln n$ .

## 4 Differentiëring en reeksen

### 4.1 Delta

#### Differenties

Differentiëring bestudeert de differentie-operator  $\Delta$ , gedefinieerd door

$$\Delta f(x) = f(x+1) - f(x)$$

Vergelijk dit met differentiaalrekening: de afgeleide-operator  $D$  is gedefinieerd door

$$Df(x) = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}$$

De belangrijkste eigenschap van  $D$  is

$$D(\lambda x \bullet x^m) = \lambda x \bullet m x^{m-1}$$

Er is een analoge eigenschap voor differenties:

$$\Delta(\lambda x \bullet x^m) = \lambda x \bullet m x^{m-1}$$

waarin

$$x^m = \prod_{j=0}^{m-1} (x-j) \quad \text{voor } m \geq 0$$

(Dit is een generalisatie van de faculteitfunctie, want  $n! = n^{\underline{n}}$ .)

### Differenties

Afleiding van de differentieformule voor  $x^m$ : voor  $m \geq 1$  is

$$\begin{aligned} & \Delta(\lambda x \bullet x^m) \\ = & \quad \{ \text{definitie van } \Delta \} \\ & \lambda x \bullet ((x+1)^m - x^m) \\ = & \quad \{ \text{definitie van } x^m \} \\ & \lambda x \bullet \left( \prod_{j=0}^{m-1} (x+1-j) - \prod_{j=0}^{m-1} (x-j) \right) \\ = & \quad \{ \text{dummytransformatie } j \leftarrow j+1 \} \\ & \lambda x \bullet \left( \prod_{j=-1}^{m-2} (x-j) - \prod_{j=0}^{m-1} (x-j) \right) \\ = & \quad \{ \text{afsplitsen } j = -1 \text{ in eerste product, } j = m-1 \text{ in tweede} \} \\ & \lambda x \bullet ((x+1) - (x-m+1)) \prod_{j=0}^{m-2} (x-j) \\ = & \quad \{ \text{rekenen; definitie van } x^m \} \\ & \lambda x \bullet m x^{m-1} \end{aligned}$$

Voor  $m = 0$  is  $x^m = 1$ , zodat de formule ook dan opgaat.

Slordigheidshalve wordt de  $\lambda x \bullet$  uit dit soort berekeningen wel eens weggelaten, maar eigenlijk is dat niet goed:  $\Delta$  werkt op functies, niet op getalwaardige expressies.

## 4.2 Differentie-sommatiestelling

### Verband met sommatie

De formule

$$\int_a^b g(x) dx = f(b) - f(a) \quad \text{als } g(x) = Df(x)$$

heeft een analogon

### Differentie-sommatiestelling

$$\sum_a^b g(x)\delta x = f(b) - f(a) \text{ als } g(x) = \Delta f(x)$$

Hierin is

$$\sum_a^b g(x)\delta x = \sum_{k=a}^{b-1} g(k)$$

Toepassing:

$$\sum_0^n x^m \delta x = \left. \frac{x^{m+1}}{m+1} \right|_0^n = \frac{n^{m+1}}{m+1}$$

### Sommen van machten

$$\begin{aligned} & \sum_{k=0}^{n-1} k \\ &= \text{\{notatie\}} \\ & \sum_0^n x^1 \delta x \\ &= \text{\{differentie-sommatiestelling\}} \\ & \frac{n^2}{2} \\ &= \text{\{definitie } n^m \text{\}} \\ & \frac{n(n-1)}{2} \end{aligned}$$

en

$$\begin{aligned} & \sum_{k=0}^{n-1} k^2 \\ &= \text{\{ } x^2 = x(x-1) + x = x^2 + x^1 \text{\}} \\ & \sum_0^n (x^2 + x^1) \delta x \\ &= \text{\{differentie-sommatiestelling\}} \\ & \frac{n^3}{3} + \frac{n^2}{2} \\ &= \text{\{definitie } n^m \text{\}} \\ & \frac{n(n-1)(n-2)}{3} + \frac{n(n-1)}{2} \end{aligned}$$

### Negatieve exponenten

We hebben

$$\begin{aligned} x^3 &= x(x-1)(x-2) \\ x^2 &= x(x-1) \\ x^1 &= x \\ x^0 &= 1 \end{aligned}$$

Als we de opeenvolgende quotiënten bekijken, lijkt het redelijk om verder te gaan met

$$\begin{aligned} x^{-1} &= \frac{1}{x+1} \\ x^{-2} &= \frac{1}{(x+1)(x+2)} \\ x^{-3} &= \frac{1}{(x+1)(x+2)(x+3)} \end{aligned}$$

dus algemeen

$$x^{-m} = \prod_{j=1}^m \frac{1}{x+j}$$

### Vermenigvuldigingswet

Algemene regel:

$$x^{m+n} = x^m(x-m)^n$$

Bewijs ingeval  $0 \leq m+n < m$ :

$$\begin{aligned} & x^m(x-m)^n \\ = & \quad \{ \text{definitie; } m > 0 \text{ en } n < 0 \} \\ & \prod_{j=0}^{m-1} (x-j) \prod_{k=1}^{-n} \frac{1}{x-m+k} \\ = & \quad \{ \text{dummytransformatie } k \leftarrow m-j \} \\ & \prod_{j=0}^{m-1} (x-j) \prod_{j=m+n}^{m-1} \frac{1}{x-j} \\ = & \quad \{ \text{domeinsplitsing; termsplitsing} \} \\ & \prod_{j=0}^{m+n-1} (x-j) \\ = & \quad \{ \text{definitie; } m+n \geq 0 \} \\ & x^{m+n} \end{aligned}$$

en analoog in de andere gevallen.

## 4.3 Analoga

### Harmonische getallen

We kunnen verifiëren dat

$$\sum_a^b x^m \delta x = \frac{x^{m+1}}{m+1} \Big|_a^b \quad \text{voor } m \neq -1$$

ook geldt voor negatieve  $m$ . Maar wat als  $m = -1$ ? Voor de corresponderende integraal is

$$\int_a^b x^{-1} dx = \ln x \Big|_a^b$$

### Harmonische getallen

Er geldt

$$\begin{aligned} & \Delta(\lambda x \bullet H_x) \\ = & \quad \{ \text{definitie van } \Delta \} \\ & \lambda x \bullet (H_{x+1} - H_x) \\ = & \quad \{ \text{definitie van } H_x \} \\ & \lambda x \bullet \left( \sum_{j=1}^{x+1} \frac{1}{j} - \sum_{j=1}^x \frac{1}{j} \right) \end{aligned}$$

$$\begin{aligned}
 &= \{ \text{splits af } j = x + 1 \} \\
 &\lambda x \bullet \frac{1}{x+1} \\
 &= \{ \text{definitie van } x^{-1} \} \\
 &\lambda x \bullet x^{-1}
 \end{aligned}$$

dus volgens de differentie-sommatiestelling is

$$\sum_a^b x^{-1} \delta x = H_x|_a^b$$

Kort gezegd:  $H_x$  is het discrete analogon van  $\ln x$ .

### De exponentiële functie

De functie  $\exp = (\lambda x \bullet e^x)$  heeft de kenmerkende eigenschap  $D \exp = \exp$ . Is er een discreet analogon, m.a.w. is er een functie  $dexp$  waarvoor  $\Delta dexp = dexp$ ?

$$\begin{aligned}
 \Delta dexp(x) &= dexp(x) \\
 \Leftrightarrow \{ \text{definitie van } \Delta \} \\
 dexp(x+1) - dexp(x) &= dexp(x) \\
 \Leftrightarrow \{ \text{rekenen} \} \\
 dexp(x+1) &= 2dexp(x)
 \end{aligned}$$

En van die recurrente betrekking is eenvoudig een oplossing te vinden:  $dexp(x) = 2^x$ .

### Differentie van een product

Is er een analogon van  $D(uv) = uDv + vDu$ ?

$$\begin{aligned}
 \Delta(uv)(x) &= \{ \text{definitie van } \Delta \} \\
 u(x+1)v(x+1) - u(x)v(x) &= \{ \text{op weg naar factor } u(x+1) - u(x) \} \\
 u(x+1)v(x+1) - u(x)v(x+1) + u(x)v(x+1) - u(x)v(x) &= \{ \text{factoren buiten haakjes halen} \} \\
 v(x+1)(u(x+1) - u(x)) + u(x)(v(x+1) - v(x)) &= \{ \text{definitie van } \Delta \} \\
 v(x+1)\Delta u(x) + u(x)\Delta v(x) &
 \end{aligned}$$

dus

$$\Delta(uv) = u\Delta v + Ev\Delta u$$

waarin

$$Ev(x) = v(x+1)$$

**Partiële sommatie**

Uit de formule voor de differentie van een product leiden we af

**Partiële sommatie**

$$\sum u\Delta v = uv - \sum v\Delta u$$

Dit kan worden gebruikt om een som te transformeren naar een gemakkelijker te berekenen som. Voorbeeld:

**Partiële sommatie**

$$\begin{aligned} & \sum_{k=0}^n k2^k \\ = & \quad \{\text{notatie}\} \\ & \sum_0^{n+1} x2^x\delta x \\ = & \quad \{\text{exponentiële functie } dexp(x) = 2^x; \Delta dexp = dexp\} \\ & \sum_0^{n+1} x\Delta dexp(x)\delta x \\ = & \quad \{\text{partiële sommatie}\} \\ & x dexp(x)|_0^{n+1} - \sum_0^{n+1} E dexp(x)\Delta(\lambda x \bullet x)(x)\delta x \\ = & \quad \{\text{substitutie van grenzen; definitie van } E; \Delta(\lambda x \bullet x) = (\lambda x \bullet 1)\} \\ & (n+1)dexp(n+1) - \sum_0^{n+1} dexp(x+1)\delta x \\ = & \quad \{\text{differentie-sommatiestelling}\} \\ & (n+1)dexp(n+1) - dexp(x+1)|_0^{n+1} \\ = & \quad \{\text{definitie } dexp; \text{substitutie van grenzen}\} \\ & (n+1)2^{n+1} - (2^{n+2} - 2) \\ = & \quad \{\text{rekenen}\} \\ & (n-1)2^{n+1} + 2 \end{aligned}$$

**Partiële sommatie**

$$\begin{aligned} & \sum_{k=0}^{n-1} kH_k \\ = & \quad \{\text{notatie}\} \\ & \sum_0^n xH_x\delta x \\ = & \quad \{\Delta(\lambda x \bullet \frac{x^2}{2}) = (\lambda x \bullet x); \text{partiële sommatie}\} \\ & H_x \frac{x^2}{2} \Big|_0^n - \sum_0^n \frac{(x+1)^2}{2} \Delta(\lambda x \bullet H_x)(x)\delta x \\ = & \quad \{\Delta(\lambda x \bullet H_x) = (\lambda x \bullet x^{-1})\} \\ & H_n \frac{n^2}{2} - \sum_0^n \frac{(x+1)^2}{2} x^{-1} \delta x \\ = & \quad \{\text{vermenigvuldigingswet: } x^{-1+2} = x^{-1}(x - (-1))^2\} \\ & H_n \frac{n^2}{2} - \sum_0^n \frac{x^2}{2} \delta x \\ = & \quad \{\text{differentie-sommatiestelling}\} \\ & H_n \frac{n^2}{2} - \frac{n^2}{4} \end{aligned}$$

**4.4 Reeksen**

**Reeksen**

Gegeven een oneindige rij  $a_0, a_1, a_2, \dots$  kunnen we de rij van partiële sommen

$$a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots$$

beschouwen. Dit noemen we een *reeks*. De reeks heet *convergent* als de partiële sommen een limiet hebben, en we schrijven dan

$$\sum_{k=0}^{\infty} a_k = \lim_{n \rightarrow \infty} \sum_{k=0}^n a_k$$

### Meetkundige reeksen

Voorbeeld: voor  $|x| < 1$  is

$$\begin{aligned} & \sum_{k=0}^{\infty} ax^k \\ = & \quad \{ \text{per definitie} \} \\ & \lim_{n \rightarrow \infty} \sum_{k=0}^n ax^k \\ = & \quad \{ \text{meetkundige rij, zie college 3} \} \\ & \lim_{n \rightarrow \infty} a \frac{1-x^{n+1}}{1-x} \\ = & \quad \{ \text{eigenschappen van lim} \} \\ & \frac{a}{1-x} (1 - \lim_{n \rightarrow \infty} x^{n+1}) \\ = & \quad \{ |x| < 1 \} \\ & \frac{a}{1-x} \end{aligned}$$

### De kosten van tellen

Bij het verzetten van een teller, bijvoorbeeld de kilometerteller van een auto, verspringen steeds een of meer cijfers. Meestal maar één, maar soms (bijvoorbeeld bij de overgang van 72999 naar 73000) meer. Hoeveel cijfers verspringen gemiddeld?

De eenhudenteller verspringt bij elke overgang, en draagt dus 1 bij aan het gemiddelde. De tientallenteller verspringt een op de 10 keer, en draagt dus  $\frac{1}{10}$  bij. De honderdtallenteller draagt op dezelfde manier  $\frac{1}{100}$  bij, enzovoort. Het gemiddelde aantal cijfers dat verspringt, is dus

$$\sum_{k=0}^{\infty} \frac{1}{10^k} = \frac{1}{1 - \frac{1}{10}} = \frac{10}{9}$$

### Absolute convergentie

#### Absolute convergentie

Als  $\sum_{k=0}^{\infty} |a_k|$  convergeert, dan convergeert ook  $\sum_{k=0}^{\infty} a_k$ . Bovendien geldt in dat geval voor elke permutatie  $p$  van  $\mathbb{N}_0$

$$\sum_{k=0}^{\infty} a_k = \sum_{k=0}^{\infty} a_{p(k)}$$

In het geval van absoluut convergente reeksen kunnen we dezelfde regels voor het manipuleren van sommen gebruiken die we voor eindige sommen geleerd hebben. Voor niet-absoluut convergente reeksen geldt dat niet: een niet-absoluut convergente reeks kan elke gewenste som krijgen door de volgorde van de termen te veranderen, en zo zelfs divergent worden.

### Termen van een convergente reeks

#### Termen van een convergente reeks

Als  $\sum_{k=0}^{\infty} a_k$  convergeert, geldt

$$\lim_{k \rightarrow \infty} a_k = 0$$

De voorwaarde  $\lim_{k \rightarrow \infty} a_k = 0$  is niet voldoende voor convergentie. Bekijk de reeks

$$\sum_{k=1}^{\infty} \frac{1}{k}$$

De partiële sommen zijn

$$\sum_{k=1}^n \frac{1}{k} = H_n \geq \ln n$$

waaruit volgt dat de reeks niet convergeert.

### Machtreeksen

Een reeks van de vorm

$$\sum_{k=0}^{\infty} a_k x^k$$

heet een *machtrees* in  $x$ .

#### Convergentiestraal

Bij elke machtrees is een  $\rho \in [0.. \infty]$  zodanig dat de reeks absoluut convergeert voor elke  $x$  met  $|x| < \rho$ . De grootste  $\rho$  met deze eigenschap heet de *convergentiestraal*.

Ingeval

$$R = \lim_{k \rightarrow \infty} \left| \frac{a_{k+1}}{a_k} \right|$$

bestaat en eindig is, geldt

$$\rho = \infty \quad \text{als } R = 0$$

$$\rho = \frac{1}{R} \quad \text{als } R \neq 0$$

### Differentiëren van een machtreeks

#### Differentiëren van een machtreeks

Laat de machtreeks  $\sum_{k=0}^{\infty} a_k x^k$  convergentiestraal  $\rho > 0$  hebben. Voor alle  $x$  met  $|x| < \rho$  is dan de functie  $f(x) = \sum_{k=0}^{\infty} a_k x^k$  differentieerbaar, en

$$Df(x) = \sum_{k=0}^{\infty} (k+1)a_{k+1}x^k$$

#### Differentiëren van een machtreeks

Voorbeeld: de machtreeks  $\sum_{k=0}^{\infty} \frac{x^k}{k!}$  heeft convergentiestraal  $\infty$ , en voor de som  $f(x)$  geldt

$$\begin{aligned} Df(x) &= \{ \text{differentiëren van een machtreeks} \} \\ &= \sum_{k=0}^{\infty} \frac{(k+1)x^k}{(k+1)!} \\ &= \{ \text{rekenen} \} \\ &= \sum_{k=0}^{\infty} \frac{x^k}{k!} \\ &= \{ \text{per definitie} \} \\ &= f(x) \end{aligned}$$

In feite geldt  $f(x) = \exp x$ .

### Taylorreeks

Een functie die door een machtreeks kan worden voorgesteld heet *analytisch* in 0. Herhaald differentiëren geeft:

#### Taylor-MacLaurin

Voor elke functie  $f$  die analytisch in 0 is, geldt

$$f(x) = \sum_{k=0}^{\infty} \frac{D^k f(0)}{k!} x^k$$

Deze reeks heet de *Taylorreeks* van de functie. Benaderingen van functies zoals  $\exp$  en  $\sin$  die we vanuit een programmeertaal aanroepen, worden meestal berekend met behulp van de Taylorreeks.

### Fourierreeks

In een machtreeks probeer je een functie te schrijven als som van termen  $1, x, x^2, x^3, \dots$ . In een *Fourierreeks* probeer je dat in termen van

$$\frac{1}{2}, \cos x, \sin x, \cos 2x, \sin 2x, \cos 3x, \sin 3x, \dots$$

op het segment  $[-\pi, \pi]$ . Een Fourierreeks heeft dus de vorm

$$\frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos kx + b_k \sin kx)$$

Vrijwel alle interessante functies blijken als Fourierreeks te schrijven te zijn, bijvoorbeeld

$$e^x = \frac{e^\pi - e^{-\pi}}{2\pi} \left( 1 - 2 \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^2 + 1} (\cos kx - k \sin kx) \right)$$

### Fourierreeks

Als een functie  $f$  een Fourierreeksontwikkeling heeft, dan zijn de coëfficiënten te bepalen als

$$a_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos kx dx$$

$$b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin kx dx$$



Benaderingen van  $f$  worden weer gevonden door een beginstuk van de Fourierreeks te gebruiken. Als de functie een beeld (bijvoorbeeld .jpg) of geluid (bijvoorbeeld .mp3) voorstelt, heeft dat het voordeel dat de hogere frequenties door het menselijk oog en oor niet goed kunnen worden waargenomen. Het verschil tussen de benadering en het origineel is dan niet merkbaar.

## 5 Afronden en afkappen

### 5.1 Floor en ceiling

#### Floor en ceiling

Conversiefuncties van reële getallen naar gehele getallen.

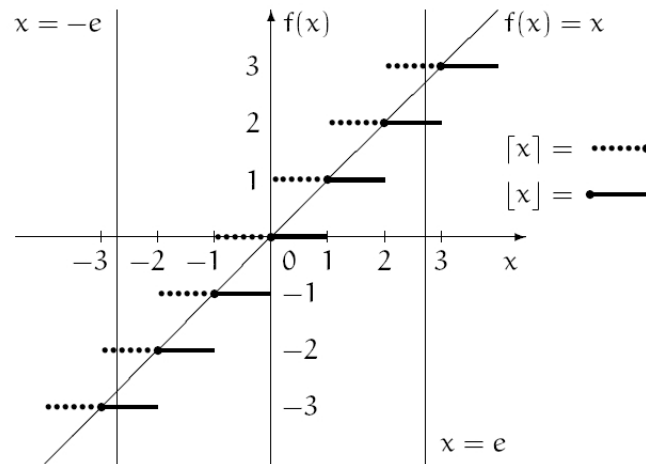
$\lfloor x \rfloor$  = het grootste gehele getal  $m$  met  $m \leq x$

$\lceil x \rceil$  = het kleinste gehele getal  $m$  met  $m \geq x$

Uitspraak:  $\lfloor x \rfloor$  als *floor*  $x$  of *entier*  $x$ , en  $\lceil x \rceil$  als *ceiling*  $x$ . Verband met typeconversie in Java:

$$(\text{int})x = \begin{cases} \lfloor x \rfloor & \text{als } x \geq 0 \\ \lceil x \rceil & \text{als } x < 0 \end{cases}$$

### Grafiek



### Rekenregels

Voor  $x \in \mathbb{R}$  en  $n \in \mathbb{Z}$  geldt

- $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$
- $\lceil x \rceil - \lfloor x \rfloor = \begin{cases} 1 & \text{als } x \notin \mathbb{Z} \\ 0 & \text{als } x \in \mathbb{Z} \end{cases}$
- $\lfloor -x \rfloor = -\lceil x \rceil$      $\lceil -x \rceil = -\lfloor x \rfloor$
- $\lfloor x \rfloor = n \iff n \leq x < n + 1$      $\lceil x \rceil = n \iff x - 1 < n \leq x$      $\lfloor x \rfloor = n \iff n - 1 < x \leq n$      $\lceil x \rceil = n \iff x \leq n < x + 1$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$      $\lceil x + n \rceil = \lceil x \rceil + n$

### Rekenregels

Voor  $x \in \mathbb{R}$  en  $n \in \mathbb{Z}$  geldt

$$\begin{aligned} x < n &\iff \lfloor x \rfloor < n \\ n < x &\iff n < \lceil x \rceil \\ x \leq n &\iff \lfloor x \rfloor \leq n \\ n \leq x &\iff n \leq \lceil x \rceil \end{aligned}$$

Bewijs (van de eerste equivalentie):

$$\begin{aligned}
& x < n \\
\Rightarrow & \{ \lfloor x \rfloor \leq x \} \\
& \lfloor x \rfloor < n \\
\Leftrightarrow & \{ \text{beide leden geheeltallig} \} \\
& \lfloor x \rfloor \leq n - 1 \\
\Rightarrow & \{ x - 1 < \lfloor x \rfloor \} \\
& x - 1 < n - 1 \\
\Leftrightarrow & \{ \text{tel 1 op bij beide leden} \} \\
& x < n
\end{aligned}$$

## Geheeltallige logaritme

### Linear search

```

int ilg(int n)
{ int k = 0;
  int t = 1;
  // invariant t = 2k
  while (t < n)
  { t*=2;
    k++;
  }
  // k minimaal met 2k ≥ n
  return k;
}

```

Dit programma berekent  $\lceil {}^2\log n \rceil$ .

### Aantal bits

Noem  $bits(n)$  het aantal bits in de binaire voorstelling van een getal  $n$ . Omdat

$$(\underbrace{1 \dots 1}_m)_2 = 2^m - 1 \quad (1)$$

geldt

$$\begin{aligned}
& bits(n) \leq m \\
\Leftrightarrow & \{ (1) \} \\
& n \leq 2^m - 1 \\
\Leftrightarrow & \{ \text{tel bij beide leden 1 op} \} \\
& n + 1 \leq 2^m \\
\Leftrightarrow & \{ \text{monotonie van } {}^2\log \} \\
& {}^2\log(n + 1) \leq m \\
\Leftrightarrow & \{ \text{eigenschap } \lceil \cdot \rceil \} \\
& \lceil {}^2\log(n + 1) \rceil \leq m
\end{aligned}$$

dus

$$\text{bits}(n) = \lceil \log_2(n+1) \rceil$$

### Wortel van floor

Te bewijzen: voor reële niet-negatieve  $x$  is  $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$ . Bewijs: voor gehele niet-negatieve  $m$  is

$$\begin{aligned} & \lfloor \sqrt{\lfloor x \rfloor} \rfloor < m \\ \Leftrightarrow & \{ \text{eigenschap van } \lfloor \cdot \rfloor \} \\ & \sqrt{\lfloor x \rfloor} < m \\ \Leftrightarrow & \{ \text{monotonie van kwadrateren} \} \\ & \lfloor x \rfloor < m^2 \\ \Leftrightarrow & \{ \text{eigenschap van } \lfloor \cdot \rfloor \} \\ & x < m^2 \\ \Leftrightarrow & \{ \text{monotonie van kwadrateren} \} \\ & \sqrt{x} < m \\ \Leftrightarrow & \{ \text{eigenschap van } \lfloor \cdot \rfloor \} \\ & \lfloor \sqrt{x} \rfloor < m \end{aligned}$$

### Integers in een interval

Gegeven een interval tussen de reële getallen  $\alpha$  en  $\beta$ , de eindpunten al dan niet daarbij ingesloten, hoeveel gehele getallen bevat dit? Voor  $\alpha < \beta$  en gehele  $n$  geldt

$$\begin{aligned} n & \in [\alpha.. \beta] \\ \Leftrightarrow & \{ \text{per definitie} \} \\ & \alpha \leq n \leq \beta \\ \Leftrightarrow & \{ \text{eigenschap van } \lfloor \cdot \rfloor \text{ en } \lceil \cdot \rceil \} \\ & \lceil \alpha \rceil \leq n \leq \lfloor \beta \rfloor \end{aligned}$$

dus het aantal gehele getallen in  $[\alpha.. \beta]$  is  $\lfloor \beta \rfloor - \lceil \alpha \rceil + 1$ . Evenzo:

$$\begin{aligned} [\alpha.. \beta] & \quad \lceil \beta \rceil - \lceil \alpha \rceil \\ (\alpha.. \beta) & \quad \lfloor \beta \rfloor - \lfloor \alpha \rfloor \\ (\alpha.. \beta) & \quad \lceil \beta \rceil - \lfloor \alpha \rfloor - 1 \end{aligned}$$

### Roulette

Een getal  $n$  met  $1 \leq n \leq 1000$  heet een winnaar als  $\lfloor \sqrt[3]{n} \rfloor \setminus n$ . Het aantal winnaars is

$$\begin{aligned} & \sum_{n=1}^{1000} \lfloor \sqrt[3]{n} \rfloor \setminus n \\ = & \{ \text{introduceer teller } k, \text{ eenpuntsregel} \} \\ & \sum_{k,n} [k = \lfloor \sqrt[3]{n} \rfloor] [k \setminus n] [1 \leq n \leq 1000] \\ = & \{ \text{introduceer teller } m, \text{ eenpuntsregel} \} \\ & \sum_{k,m,n} [k = \lfloor \sqrt[3]{n} \rfloor] [n = km] [1 \leq n \leq 1000] \\ = & \{ \text{splits af } n = 1000 \} \end{aligned}$$

$$\begin{aligned}
 & 1 + \sum_{k,m,n} [k = \lfloor \sqrt[3]{n} \rfloor] [n = km] [1 \leq n < 1000] \\
 = & \quad \{ \text{eigenschap van } \lfloor \cdot \rfloor \} \\
 & 1 + \sum_{k,m,n} [k^3 \leq n < (k+1)^3] [n = km] [1 \leq n < 1000] \\
 = & \quad \{ \text{eliminatie teller } n, \text{ eenpuntsregel} \} \\
 & 1 + \sum_{k,m} [k^3 \leq km < (k+1)^3] [1 \leq km < 1000] \\
 = & \quad \{ \text{herordenen dubbelsom, merk op } k^3 < 1000 \text{ alss } k < 10 \} \\
 & 1 + \sum_{k,m} [1 \leq k < 10] [k^2 \leq m < (k+1)^3/k] \\
 = & \quad \{ \text{aantal integers in interval} \} \\
 & 1 + \sum_k [1 \leq k < 10] ([ (k+1)^3/k ] - [k^2])
 \end{aligned}$$

### Roulette

Het aantal winnaars is

$$\begin{aligned}
 & 1 + \sum_k [1 \leq k < 10] ([ (k+1)^3/k ] - [k^2]) \\
 = & \quad \{ (k+1)^3/k = k^2 + 3k + 3 + 1/k \} \\
 & 1 + \sum_{k=1}^9 (3k + 4) \\
 = & \quad \{ \text{rekenkundige rij} \} \\
 & 1 + 9 \cdot \frac{7+31}{2} \\
 = & \quad \{ \text{rekenen} \} \\
 & 172
 \end{aligned}$$

### Asymptotische roulette

Vervang 1000 in het voorgaande door  $N$ . Dan is het aantal winnaars

$$\begin{aligned}
 & \sum_{k,m} [k^3 \leq km < (k+1)^3] [1 \leq km \leq N] \\
 = & \quad \{ \text{herordenen dubbelsom, noem } K := \lfloor \sqrt[3]{N} \rfloor \} \\
 & \sum_{k,m} [1 \leq k < K] [k^2 \leq m < (k+1)^3/k] + \sum_m [K^2 \leq m \leq N/K] \\
 = & \quad \{ \text{eerste som als voorheen; tweede via aantal integers in interval} \} \\
 & \sum_{k=1}^{K-1} (3k + 4) + (\lfloor N/K \rfloor - [K^2] + 1) \\
 = & \quad \{ \text{rekenkundige rij; } K^2 \in \mathbb{Z} \} \\
 & \frac{1}{2}(7 + 3K + 1)(K - 1) + (\lfloor N/K \rfloor - K^2 + 1) \\
 = & \quad \{ \text{rekenen} \} \\
 & \frac{1}{2}K^2 + \frac{5}{2}K - 3 + \lfloor N/K \rfloor
 \end{aligned}$$

Hierin is, voor grote waarden van  $N$ , als benadering  $\lfloor N/K \rfloor \approx N^{2/3}$  en  $\frac{1}{2}K^2 \approx \frac{1}{2}N^{2/3}$ , terwijl de andere termen van de orde van grootte van  $N^{1/3}$  of minder zijn. We schrijven het aantal winnaars als

$$\frac{3}{2}N^{2/3} + O(N^{1/3})$$

### Recurrente betrekkingen

Veel recurrente betrekkingen kunnen worden vereenvoudigd worden door floor en ceiling te gebruiken. In college 2 zagen we als formule voor  $M_n$ , het aantal vergelijkingen

nodig voor het sorteren van  $n$  elementen met Mergesort,

$$\begin{aligned}M_{2k} &= 2M_k + 2k - 1 \\M_{2k+1} &= M_k + M_{k+1} + 2k\end{aligned}$$

Dit kan eenvoudiger worden geschreven (en opgelost!) als

$$M_n = M_{\lfloor n/2 \rfloor} + M_{\lceil n/2 \rceil} + n - 1$$

In college 1 hadden we de recurrente betrekking voor het Josephus-probleem

$$\begin{aligned}J(2k) &= 2J(k) - 1 \\J(2k + 1) &= 2J(k) + 1\end{aligned}$$

wat eenvoudiger is te schrijven als

$$J(n) = 2J(\lfloor n/2 \rfloor) - (-1)^n$$

## 5.2 Geheeltallige deling

### Geheeltallige deling

Voor willekeurige  $x$  en  $y \neq 0$  noteren we

$$x \bmod y = x - y \lfloor x/y \rfloor$$

Uitspraak:  $x$  modulo  $y$ . Dit is voor positieve gehele  $x$  en  $y$  de rest bij deling van  $x$  door  $y$ , in Java genoteerd als  $x\%y$ . Bijvoorbeeld

$$\begin{aligned}5 \bmod 3 &= 2 \\5 \bmod -3 &= -1 \\-5 \bmod 3 &= 1 \\-5 \bmod -3 &= -2\end{aligned}$$

(Merk op dat in Java  $5\%(-3) == 2$  en  $(-5)\%3 == -2$ , dus bij negatieve operanden stemmen de definities niet overeen.) Voor de volledigheid definiëren we nog

$$x \bmod 0 = x$$

### Rekenregels

- $0 \leq x \bmod y < y$  als  $y > 0$   $0 \geq x \bmod y > y$  als  $y < 0$
- $x = \lfloor x \rfloor + x \bmod 1$
- $c(x \bmod y) = (cx) \bmod (cy)$

### 5.3 Sommatie

#### Tekst in kolommen

Gegeven een tekst van  $n$  regels die we in  $m$  kolommen willen verdelen.

	8	8	7	7	7
line 1	line 9	line 17	line 24	line 31	
line 2	line 10	line 18	line 25	line 32	
line 3	line 11	line 19	line 26	line 33	
line 4	line 12	line 20	line 27	line 34	
line 5	line 13	line 21	line 28	line 35	
line 6	line 14	line 22	line 29	line 36	
line 7	line 15	line 23	line 30	line 37	
line 8	line 16				

Dan zijn er  $n \bmod m$  lange kolommen, ter lengte  $\lceil n/m \rceil$ . En er zijn  $m - n \bmod m$  korte kolommen, ter lengte  $\lfloor n/m \rfloor$ .

#### Tekst in kolommen

Laat  $k$  lopen over het gebied  $0 \leq k < m$ . Dan

$$\begin{aligned}
 & \sum_k \left\lceil \frac{n-k}{m} \right\rceil \\
 = & \left\{ \text{zij } q := \lfloor n/m \rfloor \text{ en } r := n \bmod m \right\} \\
 & \sum_k \left\lceil \frac{qm+r-k}{m} \right\rceil \\
 = & \left\{ \text{rekenen} \right\} \\
 & \sum_k \left\lceil q + \frac{r-k}{m} \right\rceil \\
 = & \left\{ \text{eigenschap van } \lceil \cdot \rceil, \text{ gebruik } q \text{ geheel} \right\} \\
 & \sum_k \left( q + \left\lceil \frac{r-k}{m} \right\rceil \right) \\
 = & \left\{ \text{termsplitsing, constante term} \right\} \\
 & qm + \sum_k \left\lceil \frac{r-k}{m} \right\rceil \\
 = & \left\{ 0 \leq r < m \right\} \\
 & qm + \sum_k [k < r] \\
 = & \left\{ \text{domeinsplitsing, constante term} \right\} \\
 & qm + r \\
 = & \left\{ \text{definitie van } q \text{ en } r, \text{ definitie van mod} \right\} \\
 & n
 \end{aligned}$$

Merk op:  $\lceil \frac{n-k}{m} \rceil$  is de lengte van kolom  $k$  in het voorgaande probleem.

#### Som van wortels

Stilzwijgend laten we  $k$  en  $m$  alleen over niet-negatieve gehele getallen lopen.

$$\begin{aligned}
 & \sum_k [k < n] \lfloor \sqrt{k} \rfloor \\
 = & \left\{ \text{introduceer teller } m; \text{ eenpuntsregel} \right\} \\
 & \sum_{k,m} m [k < n] [m = \lfloor \sqrt{k} \rfloor]
 \end{aligned}$$

$$\begin{aligned}
 &= \{ \text{eigenschap } \lfloor \cdot \rfloor \} \\
 &= \sum_{k,m} m[k < n][m \leq \sqrt{k} < m+1] \\
 &= \{ \text{monotonie kwadrateren} \} \\
 &= \sum_{k,m} m[k < n][m^2 \leq k < (m+1)^2] \\
 &= \{ \text{domeinsplitsing} \} \\
 &= \sum_{k,m} m[m^2 \leq k < (m+1)^2 \leq n] + \sum_{k,m} m[m^2 \leq k < n < (m+1)^2] \\
 &= \{ \text{zij } a := \lfloor \sqrt{n} \rfloor \} \\
 &= \sum_{k,m} m[m^2 \leq k < (m+1)^2][m+1 \leq a] + \sum_{k,m} m[m = a][a^2 \leq k < n]
 \end{aligned}$$

### Som van wortels

De eerste som geeft

$$\begin{aligned}
 &= \sum_{k,m} m[m^2 \leq k < (m+1)^2][m+1 \leq a] \\
 &= \{ \text{constante term} \} \\
 &= \sum_m m((m+1)^2 - m^2)[m+1 \leq a] \\
 &= \{ \text{rekenen} \} \\
 &= \sum_m m(2m+1)[m < a] \\
 &= \{ \text{zie college 4} \} \\
 &= \sum_m (2m^2 + 3m^1)[m < a] \\
 &= \{ \text{notatie} \} \\
 &= \sum_0^a (2m^2 + 3m^1) \delta m \\
 &= \{ \text{differentie-sommatiestelling} \} \\
 &= \frac{2}{3}a^3 + \frac{3}{2}a^2 \\
 &= \{ \text{definitie van } a^i \} \\
 &= \frac{2}{3}a(a-1)(a-2) + \frac{3}{2}a(a-1) \\
 &= \{ \text{rekenen} \} \\
 &= \frac{2}{3}a^3 - \frac{1}{2}a^2 - \frac{1}{6}a
 \end{aligned}$$

### Som van wortels

De tweede som geeft

$$\begin{aligned}
 &= \sum_{k,m} m[m = a][a^2 \leq k < n] \\
 &= \{ \text{eenpuntsregel} \} \\
 &= \sum_k a[a^2 \leq k < n] \\
 &= \{ \text{constante term} \} \\
 &= a(n - a^2)
 \end{aligned}$$

Conclusie:

$$\sum_{k=0}^{n-1} \lfloor \sqrt{k} \rfloor = na - \frac{1}{3}a^3 - \frac{1}{2}a^2 - \frac{1}{6}a$$

waarin  $a = \lfloor \sqrt{n} \rfloor$ . Asymptotisch dus  $\approx \frac{2}{3}n^{3/2}$ .

## 6 Complexe getallen

### 6.1 Definitie

#### Rekenen met paren

De vergelijking  $x^2 + 1 = 0$  heeft geen oplossing in de verzameling  $\mathbb{R}$  der reële getallen (vierkantsvergelijking met negatieve discriminant). We definiëren nu een grotere verzameling waarin deze vergelijking wel opgelost kan worden.

Op de verzameling  $\mathbb{R} \times \mathbb{R}$  van geordende paren van reële getallen definiëren we een optelling en vermenigvuldiging door

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d) \\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc)\end{aligned}$$

Voor paren van de vorm  $(a, 0)$  komen de optelling en vermenigvuldiging met de gewone overeen:

$$\begin{aligned}(a, 0) + (c, 0) &= (a + c, 0) \\ (a, 0) \cdot (c, 0) &= (ac, 0)\end{aligned}$$

Een paar  $(a, 0)$  identificeren we met het reële getal  $a$ .

#### Het getal $i$

Voor het paar  $(0, 1)$  kiezen we de notatie  $i$ . Dan geldt

$$\begin{aligned}i^2 &= \{ \text{definitie van } i \} \\ &= (0, 1) \cdot (0, 1) \\ &= \{ \text{definitie van vermenigvuldiging} \} \\ &= (-1, 0) \\ &= \{ \text{identificatie van reële getallen met paren} \} \\ &= -1\end{aligned}$$

dus

$$i^2 = -1$$

#### De complexe getallen

Voor reële  $a$  en  $b$  geldt

$$\begin{aligned}a + ib &= \{ \text{identificatie van reële getallen met paren} \} \\ &= (a, 0) + (b, 0) \cdot (0, 1) \\ &= \{ \text{definitie van vermenigvuldiging} \} \\ &= (a, 0) + (0, b) \\ &= \{ \text{definitie van optelling} \} \\ &= (a, b)\end{aligned}$$

In plaats van  $(a, b)$  schrijven we voortaan gewoonlijk  $a + ib$ .

De getallen  $a + ib$  heten de complexe getallen. De verzameling van alle complexe getallen wordt aangegeven met  $\mathbb{C}$ . In  $\mathbb{C}$  heeft de vergelijking  $x^2 + 1 = 0$  wel een oplossing, namelijk  $x = i$ .

## 6.2 Rekenregels

### Rekenregels

- Optelling en vermenigvuldiging in  $\mathbb{C}$  zijn associatief ( $u(vw) = (uv)w$  etc.) en commutatief ( $uv = vu$  etc.).
- Vermenigvuldiging distribueert over optelling:

$$u(v + w) = uv + uw$$

- Er is één nulelement:

$$u + v = u \iff v = 0$$

- Er is één eenheidselement: voor  $u \neq 0$  geldt

$$uv = u \iff v = 1$$

### Tegengestelde en inverse

- Elk element heeft één tegengestelde:

$$u + v = 0 \iff u = -v$$

waarin

$$-(a + ib) = (-a) + i(-b)$$

- Elk element  $\neq 0$  heeft één inverse:

$$uv = 1 \iff u = v^{-1}$$

waarin

$$(a + ib)^{-1} = \frac{a}{a^2 + b^2} + i \frac{-b}{a^2 + b^2}$$

### Modulus en geconjugeerde

Voor een complex getal  $z = a + ib$ , waar  $a$  en  $b$  reëel, noteren we

$$\Re z = a$$

$$\Im z = b$$

$$|z| = \sqrt{a^2 + b^2}$$

$$\bar{z} = a - ib$$

Men noemt  $|z|$  de *modulus* of *absolute waarde* van  $z$ , en  $\bar{z}$  de *complex geconjugeerde* van  $z$ .

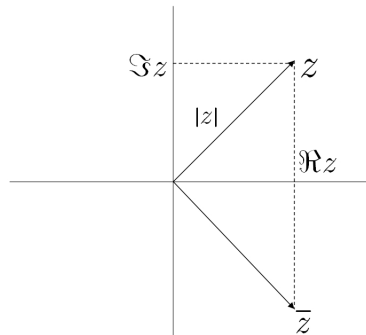
Eigenschappen:

- $z \in \mathbb{R} \iff \bar{z} = z$
- $\overline{u + v} = \bar{u} + \bar{v}$
- $\overline{uv} = \bar{u} \cdot \bar{v}$
- $|uv| = |u| \cdot |v|$
- $|u + v| \leq |u| + |v|$
- $z \cdot \bar{z} = |z|^2$
- $z + \bar{z} = 2\Re z$
- $z - \bar{z} = 2i\Im z$

### Grafische representatie

Een complex getal  $z$  kan eenvoudig grafisch worden voorgesteld door het punt in het platte vlak met  $x$ -coördinaat  $\Re z$  en  $y$ -coördinaat  $\Im z$ .

Dan stelt  $|z|$  de afstand van dit punt tot de oorsprong voor, en  $\bar{z}$  de gespiegelde ten opzichte van de  $x$ -as. Optelling van complexe getallen correspondeert met optelling van vectoren.



## 6.3 Poolcoördinaten

### Poolcoördinaten

Voor een complex getal  $z$  definiëren we  $\arg(z)$  als de unieke  $\varphi$  in  $(-\pi.. \pi]$  met

$$\Re z = |z| \cos \varphi, \quad \Im z = |z| \sin \varphi$$

In de grafische voorstelling is  $\varphi$  de hoek tussen de vector  $z$  en de positieve  $x$ -as. Dit vereenvoudigt de vermenigvuldiging:

$$\begin{aligned} & uv \\ = & \{ \text{zij } \varphi := \arg(u), \psi := \arg(v) \} \\ & (|u| \cos \varphi + i|u| \sin \varphi)(|v| \cos \psi + i|v| \sin \psi) \\ = & \{ \text{rekenen} \} \\ & |u||v| ((\cos \varphi \cos \psi - \sin \varphi \sin \psi) + i(\cos \varphi \sin \psi + \sin \varphi \cos \psi)) \end{aligned}$$

$$= \begin{matrix} \text{\{goniometrie\}} \\ |u||v| (\cos(\varphi + \psi) + i \sin(\varphi + \psi)) \end{matrix}$$

dus

$$\arg(uv) \equiv \arg(u) + \arg(v) \pmod{2\pi}$$

### Complexe $e$ -macht

Definieer, voor reële  $\varphi$ ,

$$e^{i\varphi} = \cos \varphi + i \sin \varphi$$

Deze definitie is zo gekozen dat de Taylorreeksontwikkeling

$$e^z = \sum_{k=0}^{\infty} \frac{z^k}{k!}$$

ook voor complexe  $z$  geldt. Ook belangrijke eigenschappen als

$$e^u e^v = e^{u+v}$$

$$D(\lambda z \bullet e^z) = \lambda z \bullet e^z$$

blijven dan gelden voor complexe waarden van de variabelen.

Ieder complex getal  $z$  met  $z \neq 0$  is eenduidig te schrijven in de vorm  $re^{i\varphi}$  met  $r \in (0.. \infty)$  en  $\varphi \in (-\pi.. \pi]$  (namelijk via de keuze  $r = |z|$  en  $\varphi = \arg(z)$ ).

### Complexe $e$ -macht

Voorbeelden:

- $3 + i\sqrt{3} = 2\sqrt{3}(\cos \frac{\pi}{6} + i \sin \frac{\pi}{6}) = 2\sqrt{3}e^{i\frac{\pi}{6}}$
- $\sqrt{2} + i\sqrt{2} = 2(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4}) = 2e^{i\frac{\pi}{4}}$
- $i = 0 + i = 1(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}) = e^{i\frac{\pi}{2}}$
- $-1 = -1 + i \cdot 0 = 1(\cos \pi + i \sin \pi) = e^{i\pi}$

(De formule

$$e^{i\pi} = -1$$

werd in een recente enquête als de mooiste formule uit de wiskunde gekozen.)

### Goniometrie

Goniometrische formules kunnen via complexe  $e$ -machten eenvoudig worden afgeleid (en hoeven dus niet meer van buiten geleerd of opgezocht te worden). Bijvoorbeeld:

$$\begin{aligned}
& \sin(\alpha + \beta) \\
= & \quad \{\text{definitie complexe } e\text{-macht}\} \\
& \Im e^{i(\alpha+\beta)} \\
= & \quad \{\text{rekenregel}\} \\
& \Im(e^{i\alpha}e^{i\beta}) \\
= & \quad \{\text{definitie complexe } e\text{-macht}\} \\
& \Im((\cos\alpha + i \sin \alpha)(\cos\beta + i \sin \beta)) \\
= & \quad \{\text{rekenen}\} \\
& \sin \alpha \cos \beta + \cos \alpha \sin \beta
\end{aligned}$$

## 6.4 Nulpunten

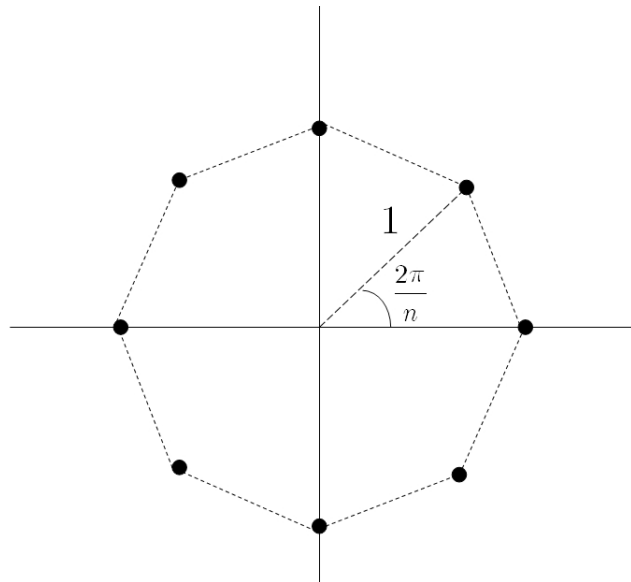
### Eenheidswortels

Onderzoek de vergelijking  $z^n = 1$  voor complexe  $z$  en natuurlijke  $n$ .

$$\begin{aligned}
& z^n = 1 \\
\Leftrightarrow & \quad \{\text{zij } r := |z|, \varphi := \arg(z)\} \\
& (re^{i\varphi})^n = 1 \\
\Leftrightarrow & \quad \{\text{rekenen}\} \\
& r^n e^{in\varphi} = 1 \\
\Leftrightarrow & \quad \{\text{modulus en argument afzonderlijk beschouwen}\} \\
& r = 1 \wedge n\varphi \equiv 0 \pmod{2\pi} \\
\Leftrightarrow & \quad \{\text{rekenen}\} \\
& r = 1 \wedge \varphi \equiv 0 \pmod{\frac{2\pi}{n}} \\
\Leftrightarrow & \quad \{-\pi < \varphi \leq \pi\} \\
& r = 1 \wedge \exists k \mid -n < 2k \leq n \bullet \varphi = \frac{2k\pi}{n} \\
\Leftrightarrow & \quad \{\text{eigenschappen van } \lfloor \cdot \rfloor \text{ en } \lceil \cdot \rceil\} \\
& r = 1 \wedge \exists k \mid -\lceil \frac{n}{2} \rceil < k \leq \lfloor \frac{n}{2} \rfloor \bullet \varphi = \frac{2k\pi}{n}
\end{aligned}$$

Het aantal oplossingen is dus  $\lceil \frac{n}{2} \rceil + \lfloor \frac{n}{2} \rfloor = n$ . Grafisch zijn dit de hoekpunten van een regelmatige  $n$ -hoek, ingeschreven in de eenheidskring.

### Eenheidswortels



**Hoofdstelling van de algebra**

**Hoofdstelling van de algebra**

Ieder polynoom

$$f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0$$

(met complexe coëfficiënten en graad  $n \geq 1$ ) is te factoriseren als

$$f(z) = (z - \omega_1)(z - \omega_2) \dots (z - \omega_n)$$

en heeft dus precies  $n$  nulpunten  $\omega_1, \dots, \omega_n$ .

De nulpunten  $\omega_j$  hoeven niet allemaal verschillend te zijn.

**Mathematica**

Invoer:

$$\text{Solve}[x^3 + 2x^2 + 3x + 12 == 0, x]$$

Uitvoer:

$$\left\{ \left\{ x \rightarrow \frac{1}{3} \left( -2 - \frac{5}{\sqrt[3]{-143 + 9\sqrt{254}}} + \sqrt[3]{-143 + 9\sqrt{254}} \right) \right\}, \right. \\ \left. \left\{ x \rightarrow -\frac{2}{3} + \frac{5(1 + i\sqrt{3})}{6\sqrt[3]{-143 + 9\sqrt{254}}} - \frac{1}{6}(1 - i\sqrt{3})\sqrt[3]{-143 + 9\sqrt{254}} \right\}, \right. \\ \left. \left\{ x \rightarrow -\frac{2}{3} + \frac{5(1 - i\sqrt{3})}{6\sqrt[3]{-143 + 9\sqrt{254}}} - \frac{1}{6}(1 + i\sqrt{3})\sqrt[3]{-143 + 9\sqrt{254}} \right\} \right\}$$

**Toepassing: recurrente betrekking**

Beschouw de recurrente betrekking

$$t_n = 2t_{n-1} - 2t_{n-2} \quad \text{voor } n \geq 2$$

met  $t_0 = 2, t_1 = 3$ . De vergelijking  $x^2 - 2x + 2 = 0$  heeft twee verschillende complexe wortels

$$\frac{2 \pm \sqrt{4 - 8}}{2} = 1 \pm i$$

Omdat

$$1 \pm i = \sqrt{2}e^{i\frac{\pi}{4}}$$

is de algemene oplossing van de recurrente betrekking van de vorm

$$t_n = C(\sqrt{2})^n \cos n\frac{\pi}{4} + D(\sqrt{2})^n \sin n\frac{\pi}{4}$$

Substitutie van de begincondities geeft

$$C = 2 \wedge C + D = 3$$

dus de gezochte oplossing is

$$t_n = 2(\sqrt{2})^n \cos n\frac{\pi}{4} + (\sqrt{2})^n \sin n\frac{\pi}{4}$$

**Mathematica**

Invoer:

```
RSolve[{t[n] == 2t[n - 1] - 2t[n - 2], t[0] == 2, t[1] == 3}, t[n], n]
```

Uitvoer:

$$\left\{ \left\{ t(n) \rightarrow 2^{n/2} \left( 2 \cos \left( \frac{n\pi}{4} \right) + \sin \left( \frac{n\pi}{4} \right) \right) \right\} \right\}$$

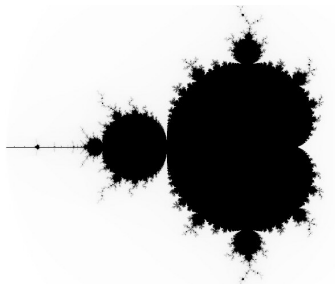
**Toepassing: Fractalen**

Beschouw de recurrente betrekking

$$z_n = z_{n-1}^2 + C \quad \text{voor } n \geq 1$$

$$z_0 = 0$$

De Mandelbrot-fractaal is de verzameling van punten  $C$  waarvoor de rij  $\lambda_n \bullet z_n$  begrensd blijft, met andere woorden: waarvoor er een  $M$  bestaat zodanig dat voor alle  $n$  geldt  $|z_n| \leq M$ . (Vergelijk practicumopdracht 1 van Imperatief Programmeren!)



## Breuksplitsing

### Breuksplitsing

Laten  $f$  en  $g$  polynomen zijn, met de graad van  $f$  kleiner dan de graad van  $g$ . Schrijf  $g$  in de vorm

$$g(z) = \prod_{j=1}^n (z - \omega_j)^{m_j}$$

waar de  $\omega_1, \dots, \omega_n$  de verschillende complexe nulpunten van  $g$  zijn. Dan zijn er constanten  $c_{j,k}$  met

$$\frac{f(z)}{g(z)} = \sum_{j=1}^n \sum_{k=1}^{m_j} \frac{c_{j,k}}{(z - \omega_j)^k}$$

### Breuksplitsing: voorbeeld

Zij  $f(z) = 3z + 1$ ,  $g(z) = z^2 + z - 6$ . Er geldt

$$g(z) = (z - 2)(z + 3)$$

dus volgens de stelling zijn er  $a$  en  $b$  met

$$\frac{3z + 1}{z^2 + z - 6} = \frac{a}{z - 2} + \frac{b}{z + 3}$$

Berekening van  $a$  en  $b$ :

$$\begin{aligned} & \forall z \mid z \neq 2 \wedge z \neq 3 \bullet \frac{3z+1}{z^2+z-6} = \frac{a}{z-2} + \frac{b}{z+3} \\ \Rightarrow & \quad \{ \text{vermenigvuldig met } z^2 + z - 6 \} \\ & \forall z \mid z \neq 2 \wedge z \neq 3 \bullet 3z + 1 = a(z + 3) + b(z - 2) \\ \Leftrightarrow & \quad \{ \text{polynomen met oneindig veel nulpunten zijn overal nul} \} \\ & \forall z \bullet 3z + 1 = a(z + 3) + b(z - 2) \\ \Rightarrow & \quad \{ \text{in het bijzonder } z = 2 \text{ en } z = -3 \} \\ & 7 = 5a \wedge -8 = -5b \\ \Leftrightarrow & \quad \{ \text{rekenen} \} \\ & a = \frac{7}{5} \wedge b = \frac{8}{5} \end{aligned}$$

### Integreren van rationale functies

Breuksplitsing is nuttig omdat we hieruit zien dat

$$\begin{aligned} & \int \frac{3z+1}{z^2+z-6} dz \\ = & \quad \{ \text{breuksplitsing} \} \\ & \frac{7}{5} \int \frac{dz}{z-2} + \frac{8}{5} \int \frac{dz}{z+3} \\ = & \quad \{ \text{elementaire integralen} \} \\ & \frac{7}{5} \ln(z - 2) + \frac{8}{5} \ln(z + 3) + C \end{aligned}$$

**Mathematica**

Invoer:

$$\text{Apart}[(3z + 1)/((z - 2)(z + 3))]$$

Uitvoer:

$$\frac{8}{5(z + 3)} + \frac{7}{5(z - 2)}$$

**7 Deelbaarheid****7.1 Deelbaarheid****Deelbaarheid**

Voor geheeltallige  $d$  en  $n$  met  $d > 0$  zeggen we dat  $d$  een *deler* is van  $n$ , en ook dat  $n$  *deelbaar* is door  $d$ , als  $\frac{n}{d}$  een geheel getal is. Notatie:

$$d \setminus n \iff \exists k : \mathbb{Z} \bullet n = kd$$

(Meer gebruikelijk, maar onhandiger, is de notatie  $d|n$ .) Eigenschappen:

- $n \setminus n$  voor  $n > 0$  (reflexiviteit)
- $d \setminus m \wedge m \setminus n \Rightarrow d \setminus n$  (transitiviteit)
- $d \setminus m \wedge d \setminus n \Rightarrow d \setminus am + bn$

**Grootste gemene deler**

De *grootste gemene deler* van  $m$  en  $n$  is het grootste natuurlijke getal dat op beide deelbaar is.

$$\text{gcd}(m, n) = \max\{d \mid d \setminus m \wedge d \setminus n\}$$

Eigenschappen:

- $\text{gcd}(m, n) = \text{gcd}(n, m)$
- $\text{gcd}(0, n) = n$  voor  $n > 0$
- $\text{gcd}(m, n) = \text{gcd}(n \bmod m, m)$

De laatstgenoemde twee eigenschappen leiden tot de *algoritme van Euclides*, die eerder al behandeld is.

**Lineairecombinatiestelling**

Belangrijke eigenschap: voor alle  $m$  en  $n$

$$\exists a, b \bullet \text{gcd}(m, n) = am + bn$$

Bewijs: inductie naar  $m$ . Basis:  $\text{gcd}(0, n) = n = 0 \cdot m + 1 \cdot n$ . Stap:

$$\begin{aligned}
& \gcd(m, n) \\
= & \quad \{ \text{eigenschap van gcd} \} \\
& \gcd(n \bmod m, m) \\
= & \quad \{ \text{inductiehypothese, gebruik } n \bmod m < m \} \\
& a(n \bmod m) + bm \\
= & \quad \{ \text{definitie van mod} \} \\
& a(n - \lfloor n/m \rfloor m) + bm \\
= & \quad \{ \text{rekenen} \} \\
& (b - a \lfloor n/m \rfloor)m + an
\end{aligned}$$

### Karakterisering van deelbaarheid

$$\begin{aligned}
& d \mid \gcd(m, n) \\
\Leftrightarrow & \quad \{ \text{definitie van gcd} \} \\
& d \mid \max\{k \mid k \mid m \wedge k \mid n\} \\
\Rightarrow & \quad \{ \text{transitiviteit van } \mid \} \\
& d \mid m \wedge d \mid n \\
\Rightarrow & \quad \{ \text{kies } a \text{ en } b \text{ volgens lineairecombinatiestelling} \} \\
& d \mid am + bn \\
\Leftrightarrow & \quad \{ \gcd(m, n) = am + bn \} \\
& d \mid \gcd(m, n)
\end{aligned}$$

dus

$$d \mid \gcd(m, n) \iff d \mid m \wedge d \mid n$$

Deze karakterisering van de functie  $\gcd$  is handiger in het gebruik dan de definitie.

## 7.2 Priemgetallen

### Priemgetallen

Een *priemgetal* is een natuurlijk getal met precies twee delers (namelijk 1 en het getal zelf). De rij priemgetallen begint met

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \dots$$

### Stelling

Elk natuurlijk getal is te schrijven als een product van priemgetallen.

Bewijs: inductie.

De basis,  $n = 1$ , is flauw: 1 is een leeg product.

Stap: als  $n$  een priemgetal is, zijn we klaar. Zo niet, dan is  $n = ab$  met  $1 < a < n$  en  $1 < b < n$ . Volgens de inductiehypothese zijn  $a$  en  $b$  het product van priemgetallen, dus  $n$  ook.  $\square$

**Uniciteit van factorisatie****Stelling**

De ontbinding in priemgetallen is uniek.

Bewijs: inductie.

De basis,  $n = 1$ , is flauw: 1 kan alleen een leeg product zijn.

Stap: zij  $n > 1$  en veronderstel  $n$  heeft twee verschillende priemfactorisaties:

$$n = p_1 p_2 \dots p_m = q_1 q_2 \dots q_k$$

Kies de naamgeving zo dat  $p_1 \leq \dots \leq p_m$  en  $q_1 \leq \dots \leq q_k$ . We gaan bewijzen uit het ongerijmde dat  $p_1 = q_1$ . Zo niet, kies de naamgeving zo dat  $p_1 < q_1$ .

**Uniciteit van factorisatie**

Omdat  $p_1$  en  $q_1$  priemgetallen zijn, is  $\gcd(p_1, q_1) = 1$ . Dus volgens de lineairecombinatiestelling zijn er  $a$  en  $b$  met

$$\begin{aligned} & ap_1 + bq_1 = 1 \\ \Rightarrow & \{ \text{vermenigvuldig met } q_2 \dots q_k \} \\ & ap_1 q_2 \dots q_k + bq_1 q_2 \dots q_k = q_2 \dots q_k \\ \Leftrightarrow & \{ q_1 \dots q_k = p_1 \dots p_m \} \\ & ap_1 q_2 \dots q_k + bp_1 p_2 \dots p_m = q_2 \dots q_k \\ \Rightarrow & \{ p_1 \text{ komt in beide termen linkerlid voor} \} \\ & p_1 \setminus q_2 \dots q_k \\ \Rightarrow & \{ \text{inductiehypothese, gebruik } q_2 \dots q_k < n \} \\ & p_1 = q_2 \vee \dots \vee p_1 = q_k \\ \Rightarrow & \{ q_1 \leq q_2 \leq \dots \leq q_k \} \\ & p_1 \geq q_1 \end{aligned}$$

en dit is in tegenspraak met de veronderstelling  $p_1 < q_1$ . Dus inderdaad  $p_1 = q_1$ . Deel deze factor weg; wegens de inductiehypothese zijn de overige factoren gelijk.  $\square$

**Mathematica**

Invoer:

```
FactorInteger[29325764]
```

Uitvoer:

```
{{2, 2}, {13, 1}, {547, 1}, {1031, 1}}
```

Dat wil zeggen:

$$29325764 = 2^2 \cdot 13 \cdot 547 \cdot 1031$$

## Het aantal priemgetallen

### Stelling (Euclides)

Er zijn oneindig veel priemgetallen.

Bewijs: uit het ongerijmde. Stel er zijn maar eindig veel priemgetallen,  $p_1, \dots, p_k$ . Beschouw het getal

$$M = p_1 \dots p_k + 1$$

Elk priemgetal is een deler van  $M-1$ , dus niet van  $M$ . Dat is in tegenspraak met de stelling dat elk natuurlijk getal het product van priemgetallen is.  $\square$

Het grootst bekende priemgetal is nu  $2^{30402457} - 1$ , een getal van 9152052 cijfers, gevonden in december 2005.

## Het aantal priemgetallen

Geef met  $\pi(x)$  het aantal priemgetallen  $\leq x$  aan.

### Priemgetalstelling

$$\pi(x) \sim \frac{x}{\ln x}, \quad x \rightarrow \infty$$

(Notatie:

$$f(x) \sim g(x), \quad x \rightarrow \infty$$

betekent

$$\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1 \quad )$$

Dit werd als vermoeden uitgesproken door Legendre in 1796. Het bewijs werd in 1896 geleverd, onafhankelijk van elkaar, door Hadamard en de la Valle-Poussin. In beide gevallen gaat het om een zeer ingewikkeld bewijs dat gebruikmaakt van complexe analyse. Een nog ingewikkelder maar 'elementair' bewijs, ter lengte van een heel boek, werd pas in 1949 geleverd.

## Onbewezen vermoedens

- **Tweelingvermoeden, ca 300 v.C.:** Er zijn oneindig veel  $n$  zo dat  $n$  en  $n + 2$  beide priem zijn.
- **Vermoeden van Goldbach, 1742:** Elk even getal groter dan 2 is te schrijven als som van twee priemgetallen.

## Ontdekken van priemgetallen

Er bestaat geen formule die gebruikt kan worden om priemgetallen te genereren. Programmatuur die priemgetallen moet produceren, werkt daarom altijd als een *zeef*: uit een verzameling getallen worden door opeenvolgende tests alle getallen geëlimineerd die geen priemgetal zijn.

De bekendste van deze methoden is de *zeef van Eratosthenes* (ca. 200 v.C.). De werking is als volgt:

1. Schrijf de natuurlijke getallen van 2 tot een zekere grens  $N$  op, noem dat de kandidatenlijst.
2. Schrap alle veelvouden van 2 uit de kandidatenlijst, te beginnen bij 4.
3. Het kleinst overgebleven getal waarvan we de veelvouden nog niet hebben geschrapt, zeg  $n$ , is een priemgetal.
4. Schrap alle veelvouden van  $n$  uit de kandidatenlijst, te beginnen bij  $n \cdot n$ .
5. Klaar als  $n \geq \lfloor \sqrt{N} \rfloor$ . Herhaal anders vanaf stap 3.

### De zeef van Eratosthenes

#### Java-methode die alle priemgetallen $< \text{limit}$ uitrekent

```
void Eratosthenes(int limit)
{ boolean[] struck = new boolean[limit];
  for (int i = 2; i < limit; i++)
    struck[i] = false;
  for (int n = 2; n*n < limit; n++)
    if (!struck[n])
      for (int i = n*n; i < limit; i += n)
        struck[i] = true;
  for (int n = 2; n < limit; n++)
    if (!struck[n]) System.out.print(n + " ");
}
```

Animatie: <http://www.cs.uu.nl/docs/vakken/wis/wis701.gif>

### Onderling ondeelbare getallen

Natuurlijke getallen  $m$  en  $n$  heten *onderling ondeelbaar* of *relatief priem* als  $\text{gcd}(m, n) = 1$ .  
 1. Notatie:  $m \perp n$ .

Eigenschappen:

- $\frac{m}{\text{gcd}(m,n)} \perp \frac{n}{\text{gcd}(m,n)}$
- $m \perp n \iff \forall p \bullet \epsilon_p(m)\epsilon_p(n) = 0$ , waarin  $\epsilon_p(n)$  de exponent van  $p$  in de priemfactorontbinding van  $n$  voorstelt
- $k \perp m \wedge k \perp n \iff k \perp mn$
- $m \perp n \iff \exists a, b \bullet am + bn = 1$

### 7.3 Congruenties

#### Congruenties modulo $m$

Zij  $m$  een vast natuurlijk getal. Beschouw de binaire relatie  $\equiv_m$ , gedefinieerd door

$$a \equiv_m b \iff a \bmod m = b \bmod m$$

De relatie  $\equiv_m$  is een *equivalentierelatie*: reflexief, symmetrisch en transitief.

Een gemakkelijker hanteerbare karakterisering is

$$a \equiv_m b \iff m \mid a - b$$

In plaats van  $a \equiv_m b$  schrijven we traditioneel

$$a \equiv b \pmod{m}$$

Het voordeel is dat de toevoeging  $\bmod(m)$  op een hele formule en alle equivalenties daarin kan slaan.

#### Rekenen met congruenties

Eigenschappen:

- $a \equiv b \wedge c \equiv d \Rightarrow a + c \equiv b + d \pmod{m}$
- $a \equiv b \wedge c \equiv d \Rightarrow a - c \equiv b - d \pmod{m}$
- $a \equiv b \wedge c \equiv d \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$
- $a \equiv b \Rightarrow a^n \equiv b^n \pmod{m}$
- $ad \equiv bd \iff a \equiv b \pmod{m}$  als  $d \perp m$

#### Chinese reststelling

##### Chinese reststelling (Sun Tsu, 350)

Als  $m \perp n$ , geldt

$$a \equiv_{mn} b \iff a \equiv_m b \wedge a \equiv_n b$$

Toepassing: multiprecisie-arithmetiek in computers. Als we willen rekenen in een interval  $[0..(p_1 p_2 \dots p_k))$  met  $p_1, \dots, p_k$  priem, dan kunnen we in plaats daarvan de berekening separaat uitvoeren voor de resten modulo elke  $p_i$ . Die laatste kunnen met de gewone integer-arithmetiek worden afgehandeld als elke  $p_i$  daarvoor klein genoeg is.

### 7.4 Euler

#### De functie van Euler

Definieer

$$\phi(n) = \#\{d \mid 0 \leq d < n \wedge d \perp n\}$$

Eigenschappen:

- $\phi(n) \leq n - 1$
- $\phi(n) = n - 1 \iff n$  priem
- $\phi$  is *multiplicatief*, d.w.z.

$$\phi(m)\phi(n) = \phi(mn) \text{ als } m \perp n$$

- $n^{\phi(m)} \equiv 1 \pmod{m}$  als  $m \perp n$

### Expliciete formule voor $\phi(p^k)$

Multiplicatieve functies worden volledig bepaald door hun waarde op de *primaire* getallen, d.w.z. getallen van de vorm  $p^k$ .

Merk eerst op dat voor  $p$  priem en  $1 \leq d < p^k$  geldt

$$d \perp p^k \iff \neg(p \mid d)$$

dus

$$\phi(p^k) = p^k - p^{k-1}$$

### Expliciete formule voor $\phi(n)$

Schrijf  $n = \prod_{p \mid n} p^{e_p}$ . Dan

$$\begin{aligned} & \phi(n) \\ = & \{ \text{ontbinding } n \} \\ & \phi\left(\prod_{p \mid n} p^{e_p}\right) \\ = & \{ \phi \text{ is multiplicatief} \} \\ & \prod_{p \mid n} \phi(p^{e_p}) \\ = & \{ \text{formule voor } \phi(p^k) \} \\ & \prod_{p \mid n} (p^{e_p} - p^{e_p-1}) \\ = & \{ \text{rekenen} \} \\ & \prod_{p \mid n} p^{e_p} \left(1 - \frac{1}{p}\right) \\ = & \{ \text{termsplitsing; ontbinding } n \} \\ & n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) \end{aligned}$$

### Sommatie van $\phi$ -waarden

Beschouw de verzameling van breuken  $\frac{m}{n}$  met  $0 \leq m < n$ . Hun aantal is  $n$ .

In elk van deze breuken kunnen we teller en noemer delen door  $\gcd(m, n)$ . De breuk krijgt dan de vorm  $\frac{c}{d}$  met  $c \perp d$ ; en elke breuk van deze vorm met  $d \mid n$  is zo verkregen (uit de oorspronkelijke  $\frac{m}{n}$ , waar  $m = c \frac{n}{d}$ ).

Het aantal zulke breuken met noemer  $d$  is  $\phi(d)$ . Hieruit zien we

$$n = \sum_{d \mid n} \phi(d)$$

## 7.5 RSA

### RSA

RSA is een algoritme voor *public-key encryption*, bedacht in 1977 door Ron Rivest, Adi Shamir en Len Adleman (MIT).

Dit is een methode om versleutelde berichten zodanig te verzenden dat geen geheime overdracht van sleutels nodig is.

Elke gebruiker van RSA kiest twee sleutels. De openbare sleutel wordt door de buitenwereld gebruikt om berichten aan de gebruiker te versleutelen, de priv sleutel wordt door de gebruiker gebruikt om die berichten te ontsleutelen.

### Genereren van sleutels

1. Kies twee verschillende grote priemgetallen  $p$  en  $q$
2. Bereken  $n = pq$
3. Bereken  $\phi(n) = (p - 1)(q - 1)$
4. Kies een  $e$  met  $1 < e < \phi(n)$  met  $e \perp \phi(n)$
5. Kies  $d$  met  $de \equiv 1 \pmod{\phi(n)}$

De openbare sleutel bestaat uit  $n$  en  $e$  (van *encryptie*), de priv sleutel uit  $d$  (van *decryptie*).

### Encryptie en decryptie

Gegeven een bericht  $m$  (van *message*), met  $2 \leq m < n$ . Daaruit wordt de versleutelde vorm  $c$  (van *ciphertext*) berekend door

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

Omgekeerd wordt uit  $c$  een boodschap  $m'$  berekend door

$$m' = c^d \pmod{n}$$

### Encryptie en decryptie

Claim:  $m' = m$ . Bewijs:

$$\begin{aligned} & m' = m \\ \Leftrightarrow & \{ 0 \leq m' < n \text{ en } 2 \leq m < n \} \\ & m' \equiv_n m \\ \Leftrightarrow & \{ \text{definitie van } m' \} \\ & c^d \equiv_n m \\ \Leftrightarrow & \{ \text{definitie van } c \} \\ & (m^e)^d \equiv_n m \\ \Leftrightarrow & \{ \text{Chinese reststelling, } n = pq \text{ en } p \perp q \} \\ & m^{ed} \equiv_p m \wedge m^{ed} \equiv_q m \end{aligned}$$

**Encryptie en decryptie**

Voor de termen in de laatste regel geldt

$$\begin{aligned}
 & m^{ed} \equiv_p m \\
 \Leftarrow & \{ ed \equiv_{\phi(p)} 1 \} \\
 & m \cdot m^{\phi(p)} \equiv_p m \\
 \Leftarrow & \{ \text{vermenigvuldiging van congruenties} \} \\
 & m \equiv_p 0 \vee m^{\phi(p)} \equiv_p 1 \\
 \Leftarrow & \{ \text{eerder genoemde eigenschappen van } \equiv_p \text{ resp. } \phi \} \\
 & p \nmid m \vee p \perp m
 \end{aligned}$$

en dit laatste is inderdaad het geval omdat  $p$  een priemgetal is. Dezelfde redenering geldt voor  $q$ .

**8 Vectoren**

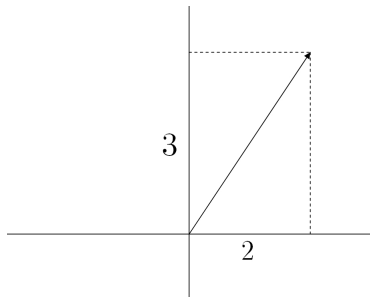
**8.1 Vectoren**

**Vectoren**

Een *vector* met dimensie 2 is een kolom bestaande uit twee reële getallen, bijvoorbeeld

$$\begin{bmatrix} 2 \\ 3 \end{bmatrix}$$

We kunnen deze meetkundig interpreteren als een pijl in het platte vlak van de oorsprong naar het punt  $(2, 3)$ . De verzameling van alle vectoren met dimensie 2 geven we aan met  $\mathbb{R}^2$ . Analoog definiëren we  $\mathbb{R}^3$ , meetkundig te interpreteren als een pijl in de driedimensionale ruimte.



Toepassingen in de natuurkunde: snelheden, versnellingen, krachten.

**Vectoren**

Meer algemeen kunnen we  $\mathbb{R}^n$  beschouwen als de verzamelingen van kolommen van  $n$  reële getallen. Er is dan geen aanschouwelijke meetkundige interpretatie. Analoog ook  $\mathbb{C}^n$ .

Toepassing: een muziekstuk van 180 seconden met een samplerate van 44100/s is een punt in  $\mathbb{R}^{7938000}$ .

### Optellen van vectoren

De *som* van twee vectoren wordt berekend door het optellen van de overeenkomstige componenten, bijvoorbeeld

$$\begin{bmatrix} 2 \\ 6 \\ 0 \end{bmatrix} + \begin{bmatrix} -3 \\ 5 \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} -1 \\ 11 \\ \frac{1}{2} \end{bmatrix}$$

Meetkundig is dit de diagonaal van het parallellogram opgespannen door de twee vectoren.

Dit stemt overeen met de natuurkundige interpretatie van de resultante van verschillende krachten, en is analoog aan de optelling van complexe getallen. (In het muziekvoorbeeld: digitaal mixen van muziek.)

Deze optelling is commutatief:  $\vec{x} + \vec{y} = \vec{y} + \vec{x}$ .

### Scalair product

Voor een reëel getal  $\alpha$  en een vector  $\vec{x}$  definiëren we het scalaire product  $\alpha\vec{x}$  door elke component van  $\vec{x}$  met  $\alpha$  te vermenigvuldigen, bijvoorbeeld

$$2 \begin{bmatrix} 3 \\ 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 6 \\ 10 \\ 2 \end{bmatrix}$$

(In het muziekvoorbeeld is dit de volumeregelaar.) Eigenschappen:

- $\alpha(\vec{x} + \vec{y}) = \alpha\vec{x} + \alpha\vec{y}$
- $(\alpha + \beta)\vec{x} = \alpha\vec{x} + \beta\vec{x}$
- $\alpha(\beta\vec{x}) = (\alpha\beta)\vec{x}$

In plaats van  $(-1)\vec{x}$  schrijven we  $-\vec{x}$ . In plaats van  $0\vec{x}$  schrijven we  $\vec{0}$ , de *nulvector*. Eigenschappen:

- $-\vec{x} + \vec{x} = \vec{0}$
- $\vec{x} + \vec{0} = \vec{x}$

## 8.2 Lineaire combinaties

### Lineaire combinaties

Een *lineaire combinatie* van de vectoren  $\vec{x}_1, \dots, \vec{x}_m$  is een uitdrukking van de vorm

$$\alpha_1\vec{x}_1 + \alpha_2\vec{x}_2 + \dots + \alpha_m\vec{x}_m$$

De vectoren  $\vec{x}_1, \dots, \vec{x}_m$  heten *onafhankelijk* als de nulvector niet te schrijven is als een niet-triviale lineaire combinatie ervan, dus als

$$\alpha_1\vec{x}_1 + \alpha_2\vec{x}_2 + \dots + \alpha_m\vec{x}_m = \vec{0} \iff \alpha_1 = \alpha_2 = \dots = \alpha_m = 0$$

Voorbeeld: de vectoren

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

zijn afhankelijk. Meetkundige interpretatie: de drie pijlen liggen in één vlak.

### Bases

Een stel vectoren  $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m$  uit  $\mathbb{R}^n$  heet een *stel voortbrengers* van  $\mathbb{R}^n$  als iedere vector uit  $\mathbb{R}^n$  te schrijven is als lineaire combinatie ervan.

Een stel vectoren  $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m$  uit  $\mathbb{R}^n$  heet een *basis* van  $\mathbb{R}^n$  als geldt

1.  $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m$  is een stel voortbrengers van  $\mathbb{R}^n$
2.  $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m$  is onafhankelijk

Een basis voor  $\mathbb{R}^2$  is

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Dit heet de *standaardbasis*, gewoonlijk aangeduid als  $\vec{e}_1, \vec{e}_2$ .

### Lineaire vergelijkingen

Om te onderzoeken of

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

een basis vormt van  $\mathbb{R}^2$ , moeten we laten zien dat de vergelijking

$$\alpha \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \beta \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

alleen de nuloplossing heeft, en dat de vergelijking

$$\alpha \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \beta \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}$$

voor elke  $u, v$  een oplossing heeft.

### Lineaire vergelijkingen

Het eerste stelsel is te schrijven als

$$\alpha + \beta = 0$$

$$\alpha - \beta = 0$$

Optellen geeft  $2\alpha = 0$  dus  $\alpha = 0$ . Substitutie in de eerste vergelijking geeft  $\beta = 0$ .

Het tweede stelsel is te schrijven als

$$\alpha + \beta = u$$

$$\alpha - \beta = v$$

Optellen geeft  $2\alpha = u + v$  dus  $\alpha = \frac{1}{2}(u + v)$ . Aftrekken geeft  $2\beta = u - v$  dus  $\beta = \frac{1}{2}(u - v)$ . Door substitutie zien we dat hiermee aan beide vergelijkingen is voldaan.

**Alternatieve basis**

Conclusie:

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

is ook een basis van  $\mathbb{R}^2$ .

Toepassing: Deze basis wordt gebruikt in FM-stereo-uitzendingen, waar niet het linker- en rechtergeluid apart worden verzonden, maar een monosignaal  $M = L + R$  en een stereoverschilsignaal  $S = L - R$ . (Deze signaaldefinitie zorgt namelijk voor compatibiliteit tussen mono- en stereoapparatuur.)

**Dimensie****Stelling**

Een stel vectoren  $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m$  uit  $\mathbb{R}^n$  is een *basis* van  $\mathbb{R}^n$  als geldt

1.  $m = n$
2.  $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_m$  is onafhankelijk

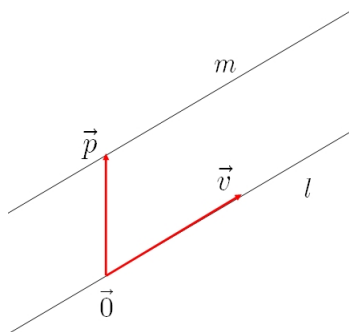
Alle bases van de ruimte hebben dus evenveel elementen. Dit aantal heet de *dimensie* van de ruimte.

**8.3 Lijn en vlak****Vectorvoorstelling van een lijn**

Als  $l$  een lijn door de oorsprong is en  $\vec{v}$  een vector waarvan het eindpunt op  $l$  ligt, dan is iedere vector  $\vec{x}$  waarvan het eindpunt op  $l$  ligt (maar niet  $\vec{0}$  is) te schrijven in de vorm  $\vec{x} = \alpha\vec{v}$ , en omgekeerd. We noemen  $\vec{x} = \alpha\vec{v}$  een *vectorvoorstelling* van de lijn  $l$ . Zij nu  $m$  een lijn die niet door de oorsprong gaat. Beschouw de lijn  $l$  door de oorsprong evenwijdig aan  $m$ . Laat  $\vec{x} = \alpha\vec{v}$  de vectorvoorstelling van  $l$  zijn. Zij  $\vec{p}$  een vector waarvan het eindpunt op  $m$  ligt. Dan is elke vector  $\vec{x}$  waarvan het eindpunt op  $m$  ligt te schrijven in de vorm

$$\vec{x} = \vec{p} + \alpha\vec{v}$$

We noemen  $\vec{v}$  in deze vectorvoorstelling de *richtingsvector* en  $\vec{p}$  de *steunvector*.



**Vectorvoorstelling en vergelijking**

Beschouw de lijn  $m$  in het platte vlak met vergelijking  $x + 3y = 4$ . Twee oplossingen zijn  $(1, 1)$  en  $(4, 0)$ . De vectoren

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix}$$

hebben dus hun eindpunt op  $m$ , en hun verschil  $\begin{bmatrix} -3 \\ 1 \end{bmatrix}$  is evenwijdig met  $m$ . Een vectorvoorstelling van  $m$  is dus bijvoorbeeld

$$\vec{x} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \alpha \begin{bmatrix} -3 \\ 1 \end{bmatrix}$$

**Vectorvoorstelling van een vlak**

Als het vlak  $V$  door de oorsprong gaat en  $\vec{u}, \vec{v}$  een stel *onafhankelijke* vectoren is waarvan de eindpunten in  $V$  liggen, dan is elke vector met eindpunt in  $V$  te schrijven als lineaire combinatie van  $u$  en  $v$ . Een vectorvoorstelling van  $V$  is dan

$$\vec{x} = \alpha\vec{u} + \beta\vec{v}$$

Zij nu  $W$  een vlak dat niet door de oorsprong gaat. Beschouw het vlak  $V$  door de oorsprong evenwijdig aan  $W$ . Laat  $\vec{x} = \alpha\vec{u} + \beta\vec{v}$  een vectorvoorstelling van  $V$  zijn. Zij  $\vec{p}$  een vector waarvan het eindpunt op  $W$  ligt. Dan is elke vector  $\vec{x}$  waarvan het eindpunt op  $W$  ligt te schrijven in de vorm

$$\vec{x} = \vec{p} + \alpha\vec{u} + \beta\vec{v}$$

We noemen  $\vec{u}$  en  $\vec{v}$  hierin de richtingsvectoren. (Als  $\vec{u}$  en  $\vec{v}$  afhankelijk zijn (maar niet  $\vec{0}$ ), beschrijft deze vectorvoorstelling op nodeloos ingewikkelde wijze een lijn.)

**8.4 Norm en inproduct****Norm**

De *norm* van een vector  $\vec{x}$  in  $\mathbb{R}^n$ , genoteerd  $|\vec{x}|$ , is als volgt gedefinieerd: de norm van

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

is

$$\sqrt{\sum_{i=1}^n x_i^2}$$

Bijvoorbeeld

$$\left| \begin{bmatrix} 2 \\ 3 \end{bmatrix} \right| = \sqrt{2^2 + 3^2} = \sqrt{13}$$

In de meetkundige interpretatie is dit de lengte van de pijl. (In de natuurkundige interpretatie de grootte van de snelheid, kracht etc. met verwaarlozing van de richting.)

**Inproduct**

Het *inproduct* van vectoren  $\vec{x}, \vec{y}$  in  $\mathbb{R}^n$ , genoteerd  $\vec{x} \cdot \vec{y}$ , is als volgt gedefinieerd:

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \sum_{i=1}^n x_i y_i$$

Gevolg:

$$|\vec{x}| = \sqrt{\vec{x} \cdot \vec{x}}$$

Meetkundige interpretatie:

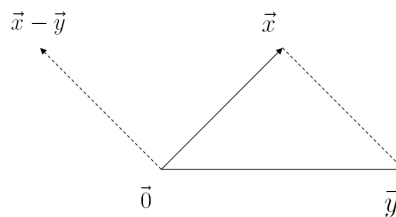
$$\vec{x} \cdot \vec{y} = |\vec{x}| |\vec{y}| \cos \phi$$

waar  $\phi$  de hoek tussen de vectoren  $\vec{x}$  en  $\vec{y}$  is.

**Inproduct**

Uitleg van de meetkundige interpretatie:

$$\begin{aligned} & |\vec{x} - \vec{y}|^2 \\ = & \quad \{\text{definitie van norm}\} \\ & \sum_i (x_i - y_i)^2 \\ = & \quad \{\text{rekenen}\} \\ & \sum_i (x_i^2 + y_i^2 - 2x_i y_i) \\ = & \quad \{\text{termsplitsing}\} \\ & \sum_i x_i^2 + \sum_i y_i^2 - 2 \sum_i x_i y_i \\ = & \quad \{\text{definitie van norm en inproduct}\} \\ & |\vec{x}|^2 + |\vec{y}|^2 - 2\vec{x} \cdot \vec{y} \end{aligned}$$



Anderzijds, wegens de cosinusregel,

$$|\vec{x} - \vec{y}|^2 = |\vec{x}|^2 + |\vec{y}|^2 - 2|\vec{x}| |\vec{y}| \cos \phi$$

**Mathematica**

Invoer:

$$\text{Norm}[\{1, 5, 12\}]$$

Uitvoer:

$$\sqrt{170}$$

Invoer:

$$\{1, 5, 12\}, \{2, -1, -2\}$$

Uitvoer:

$$-27$$

**Berekenen van de hoek tussen vectoren**

Gevraagd de hoek te berekenen tussen de vectoren

$$\vec{x} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \quad \vec{y} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Oplossing:

$$\begin{aligned} |\vec{x}| &= \sqrt{1^2 + 1^2 + 1^2} = \sqrt{3} \\ |\vec{y}| &= \sqrt{1^2 + 0^2 + 0^2} = 1 \\ \vec{x} \cdot \vec{y} &= 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 = 1 \end{aligned}$$

dus voor de gevraagde hoek  $\phi$  geldt

$$\cos \phi = \frac{1}{\sqrt{3}}$$

Mathematica: invoer `ArcCos[1/Sqrt[3]]/Degree//N` geeft uitvoer 54.7356, dus de gevraagde hoek is  $\approx 54.7356$  graden.

**Toepassing: ISBN**

Het ISBN (Internationaal Standaard Boeknummer) bestond tot 1 januari 2007 uit 10 cijfers, sindsdien uit 13 cijfers. Het laatste cijfer is een controlecijfer. Voor een boek dat al een tiencijferig ISBN had, is de 13-cijferige versie gelijk aan '978' gevolgd door de eerste negen cijfers van het oude ISBN. Het controlecijfer wordt in beide gevallen echter anders berekend.

Voor de 10-cijferversie gaat de berekening van het controlecijfer als volgt. Zij  $\vec{x}$  in  $\mathbb{R}^9$  de vector met de eerste 9 cijfers van het ISBN als componenten. Zij  $\vec{y}$  de vaste vector

$$\begin{bmatrix} 1 \\ 2 \\ \vdots \\ 9 \end{bmatrix}$$

Formeel is dus  $\vec{y} = [i]_{i=1}^9$ .

**Toepassing: ISBN**

Definieer

$$n = (\vec{x} \cdot \vec{y}) \bmod 11$$

Dan is het laatste cijfer gelijk aan  $n$  als  $0 \leq n < 10$ , aan  $X$  als  $n = 10$ . Voorbeeld: ISBN 0-201-55802-? geeft in Mathematica invoer

$$\text{Mod}[\{0, 2, 0, 1, 5, 5, 8, 0, 2\} \cdot \{1, 2, 3, 4, 5, 6, 7, 8, 9\}, 11]$$

en uitvoer 5.

**Toepassing: ISBN**

Voor de 13-cijfersversie is de berekening als volgt. Zij  $\vec{a}$  in  $\mathbb{R}^{12}$  de vector met de eerste 12 cijfers van het ISBN als componenten. Zij  $\vec{b}$  de vaste vector

$$\begin{bmatrix} 1 \\ 3 \\ 1 \\ 3 \\ \vdots \end{bmatrix}$$

Formeel is  $\vec{b} = [1 + 2((i - 1) \bmod 2)]_{i=1}^{12}$ . Nu is het laatste cijfer gelijk aan

$$(10 - (\vec{a} \cdot \vec{b}) \bmod 10) \bmod 10$$

Voorbeeld: ISBN 978-0-201-55802-? geeft in Mathematica invoer

$$\text{Mod}[10 - \text{Mod}[\{9, 7, 8, 0, 2, 0, 1, 5, 5, 8, 0, 2\} \cdot \{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3\}, 10], 10]$$

en uitvoer 9.

(Al voor de officiële invoering van ISBN-13 werd dezelfde formule gebruikt voor de berekening van het controlecijfer in de streepjescodes die op veel boeken worden afgebeeld.)

**Normaalvectoren**

Twee vectoren staan loodrecht op elkaar als en alleen als hun inproduct 0 is. Een vector die loodrecht staat op de richtingsvectoren van een vlak of lijn heet een *normaalvector* daarvan.

Beschouw de lijn in het platte vlak met vergelijking  $2x + 3y = 0$ . Deze vergelijking is te schrijven als

$$\begin{bmatrix} 2 \\ 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = 0$$

De punten  $(x, y)$  op de lijn worden dus gekarakteriseerd door de uitspraak dat de vector  $\begin{bmatrix} x \\ y \end{bmatrix}$  loodrecht staat op  $\begin{bmatrix} 2 \\ 3 \end{bmatrix}$ . Dus laatstgenoemde is een normaalvector van de lijn, en als richtingsvector kunnen we een vector loodrecht daarop kiezen, bijvoorbeeld  $\begin{bmatrix} 3 \\ -2 \end{bmatrix}$ .

## 9 Matrixrekening

### 9.1 Vergelijkingen

#### Stelsels lineaire vergelijkingen

Een stelsel van  $m$  lineaire vergelijkingen in de  $n$  onbekenden  $x_1, x_2, \dots, x_n$  is een stelsel vergelijkingen van de vorm

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \dots + a_{m,n}x_n &= b_m \end{aligned}$$

We kunnen dit verkort opschrijven als

$$A\vec{x} = \vec{b}$$

waarin

$$\vec{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad \vec{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

en  $A$  de *matrix* van coëfficiënten is.

#### Matrices

De matrix  $A$  noteren we als

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & & & \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{bmatrix}$$

of kort als  $[a_{i,j}]_{i,j=1}^{m,n}$ .

We spreken van een  $m \times n$ -matrix (eerst de rij-index, dan de kolom-index).

#### Product van een matrix en een vector

Het *product* van een matrix  $[a_{i,j}]_{i,j=1}^{m,n}$  en een vector  $[x_j]_{j=1}^n$  is gedefinieerd als de vector

$$\left[ \sum_{j=1}^n a_{i,j}x_j \right]_{i=1}^m$$

(Merk op: sommatie over dubbel voorkomende index (Einstein-conventie).) Met andere woorden:

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & & & \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n \\ a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \dots + a_{m,n}x_n \end{bmatrix}$$

Met deze afspraak is het oorspronkelijke stelsel vergelijkingen inderdaad te schrijven als  $A\vec{x} = \vec{b}$ .

## 9.2 Matrixvermenigvuldiging

### Matrixvermenigvuldiging

We kunnen een vector opvatten als een matrix met breedte 1. Het product van een matrix en een vector is dan te generaliseren tot willekeurige matrices.

Het *product*  $AB$  van twee matrices is gedefinieerd als de breedte van  $A$  gelijk is aan de hoogte van  $B$ , en wel als volgt: als  $A = [a_{i,j}]_{i,j=1,1}^{m,n}$  en  $B = [b_{j,k}]_{j,k=1,1}^{n,l}$ , dan geldt

$$AB = \left[ \sum_{j=1}^n a_{i,j} b_{j,k} \right]_{i,k=1,1}^{m,l}$$

Merk op dat het element op plaats  $i, k$  in  $AB$  het inproduct van rij  $i$  in  $A$  en kolom  $k$  in  $B$  is.

### Matrixvermenigvuldiging

Voorbeeld:

$$\begin{aligned} & \begin{bmatrix} 3 & 1 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} -1 & 4 & 0 \\ 2 & -1 & 5 \end{bmatrix} \\ = & \quad \{\text{matrixvermenigvuldiging}\} \\ & \begin{bmatrix} 3 \cdot (-1) + 1 \cdot 2 & 3 \cdot 4 + 1 \cdot (-1) & 3 \cdot 0 + 1 \cdot 5 \\ 2 \cdot (-1) + 0 \cdot 2 & 2 \cdot 4 + 0 \cdot (-1) & 2 \cdot 0 + 0 \cdot 5 \end{bmatrix} \\ = & \quad \{\text{rekenen}\} \\ & \begin{bmatrix} -1 & 11 & 5 \\ -2 & 8 & 0 \end{bmatrix} \end{aligned}$$

Mathematica: invoer (vergeet infix dot niet!):

$$\{\{3, 1\}, \{2, 0\}\} \cdot \{\{-1, 4, 0\}, \{2, -1, 5\}\}$$

Uitvoer:

$$\{\{-1, 11, 5\}, \{-2, 8, 0\}\}$$

### Eigenschappen van vermenigvuldiging

- Matrixvermenigvuldiging is *niet* commutatief!

$$\begin{aligned} \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 1 & 2 \end{bmatrix} &= \begin{bmatrix} 3 & 8 \\ 1 & 6 \end{bmatrix} \\ \begin{bmatrix} -1 & 0 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix} &= \begin{bmatrix} -1 & -4 \\ 5 & 10 \end{bmatrix} \end{aligned}$$

- Matrixvermenigvuldiging is wel associatief: voor een  $(m \times n)$ -matrix  $A$ , een  $(n \times l)$ -matrix  $B$  en een  $(l \times k)$ -matrix  $C$  geldt  $(AB)C = A(BC)$ .
- De vermenigvuldiging van vierkante matrices van dimensie  $n$  heeft als eenheidselement de matrix  $I_n = [[i = j]]_{i,j=1,1}^{n,n}$ . D.w.z. voor een  $(n \times n)$ -matrix  $A$  is  $AI_n = I_nA = A$ .
- De vermenigvuldiging van vierkante matrices van dimensie  $n$  heeft als nulelement de matrix  $0_n = [0]_{i,j=1,1}^{n,n}$ . D.w.z. voor een  $(n \times n)$ -matrix  $A$  is  $A0_n = 0_nA = 0_n$ .

### Matrixinversie

Voor elke  $(n \times n)$ -matrix  $A$  bestaat er ten hoogste één  $(n \times n)$ -matrix  $B$  met

$$AB = BA = I_n$$

We kunnen zelfs iets sterkers bewijzen: als  $AB = CA = I_n$ , dan  $B = C$ . Immers,

$$\begin{aligned} B &= C \\ \Leftrightarrow \{ I_n \text{ is eenheidselement van vermenigvuldiging} \} \\ I_n B &= C I_n \\ \Leftrightarrow \{ AB = I_n \text{ en } CA = I_n \} \\ CAB &= CAB \end{aligned}$$

De matrix  $B$  wordt, als hij bestaat, aangegeven met  $A^{-1}$  en de *inverse* matrix genoemd.

## 9.3 Determinant

### Determinant van een $2 \times 2$ -matrix

Voor een  $2 \times 2$ -matrix  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  definiëren we de *determinant* als

$$\det A = ad - bc$$

Dan geldt:  $A$  heeft een inverse als en alleen als  $\det A \neq 0$ , en de inverse is gelijk aan

$$\frac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

### Determinant van een $2 \times 2$ -matrix

Voorbeeld: beschouw de matrix  $A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}$ . De determinant is  $\det A = 2 \cdot 3 - 5 \cdot 1 = 1$ .

De inverse is dus  $A^{-1} = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$ .

We kunnen de inverse matrix gebruiken om stelsels lineaire vergelijkingen snel op te lossen. Het stelsel vergelijkingen

$$\begin{aligned} 2x_1 + 5x_2 &= 11 \\ x_1 + 3x_2 &= 6 \end{aligned}$$

kan worden geschreven als  $A\vec{x} = \begin{bmatrix} 11 \\ 6 \end{bmatrix}$ .

### Oplossen van vergelijkingen met matrixinversie

De vergelijking  $A\vec{x} = \begin{bmatrix} 11 \\ 6 \end{bmatrix}$  heeft als oplossing

$$\begin{aligned} & \vec{x} \\ = & \quad \{ \text{vermenigvuldig de vergelijking links met } A^{-1} \} \\ & A^{-1} \begin{bmatrix} 11 \\ 6 \end{bmatrix} \\ = & \quad \{ \text{substitueer } A^{-1} \} \\ & \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 11 \\ 6 \end{bmatrix} \\ = & \quad \{ \text{matrixvermenigvuldiging} \} \\ & \begin{bmatrix} 3 \cdot 11 + (-5) \cdot 6 \\ (-1) \cdot 11 + 2 \cdot 6 \end{bmatrix} \\ = & \quad \{ \text{rekenen} \} \\ & \begin{bmatrix} 3 \\ 1 \end{bmatrix} \end{aligned}$$

### Oplossen van vergelijkingen door vegen

De voorgaande methode helpt alleen als we de inverse matrix kennen. Bij  $2 \times 2$ -matrices is die gemakkelijk uit te rekenen, bij hogere dimensie is het echter niet minder werk dan het rechtstreeks oplossen van de vergelijkingen door successieve eliminatie – tenzij we Mathematica gebruiken.

De oplossingsmethode door successieve eliminatie kan in matrixnotatie compact worden genoteerd. We spreken dan van ‘vegen’.

$$\begin{aligned} & \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \vec{x} = \begin{bmatrix} 11 \\ 6 \end{bmatrix} \\ \Leftrightarrow & \quad \{ \text{vegen met tweede rij} \} \\ & \begin{bmatrix} 0 & -1 \\ 1 & 3 \end{bmatrix} \vec{x} = \begin{bmatrix} -1 \\ 6 \end{bmatrix} \\ \Leftrightarrow & \quad \{ \text{vegen met eerste rij} \} \\ & \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \vec{x} = \begin{bmatrix} -1 \\ 3 \end{bmatrix} \\ \Leftrightarrow & \quad \{ \text{matrixvermenigvuldiging} \} \\ & x_1 = 3 \wedge x_2 = 1 \end{aligned}$$

### Inverse van een $n \times n$ -matrix

Voor een  $n \times n$ -matrix  $A = [a_{i,j}]_{i,j=1}^{n,n}$  voeren we de volgende notatie in:  $A_{i,j}$  is de  $(n-1) \times (n-1)$ -matrix die ontstaat door uit  $A$  de  $i$ -de rij en de  $j$ -de kolom weg te laten.

Met deze notatie kunnen we de determinant definiëren als

$$\det A = \sum_{i=1}^n (-1)^{i+1} a_{i,1} \det A_{i,1}$$

Indien  $\det A \neq 0$ , is de inverse

$$A^{-1} = \left[ (-1)^{i+j} \frac{\det A_{j,i}}{\det A} \right]_{i,j=1,1}^{n,n}$$

Dit stemt met de eerdere regels overeen voor  $n = 2$  als we de determinant van een  $1 \times 1$ -matrix  $[a]$  gelijkstellen met  $a$ .

We wijzen erop dat bovenstaande expliciete formule voor de inverse matrix niet een efficiënte manier vormt om de inverse matrix uit te rekenen.

### Determinant van een $3 \times 3$ -matrix

$$\begin{aligned} & \det \begin{bmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \\ 2 & 3 & 5 \end{bmatrix} \\ = & \quad \{\text{definitie van determinant}\} \\ & 1 \cdot \det \begin{bmatrix} 0 & 1 \\ 3 & 5 \end{bmatrix} - (-1) \cdot \det \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} + 2 \cdot \det \begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix} \\ = & \quad \{\text{determinant van de } 2 \times 2\text{-matrices}\} \\ & 1 \cdot (0 \cdot 5 - 3 \cdot 1) - (-1) \cdot (2 \cdot 5 - 3 \cdot 3) + 2 \cdot (2 \cdot 1 - 0 \cdot 3) \\ = & \quad \{\text{rekenen}\} \\ & 2 \end{aligned}$$

Dit heet ‘ontwikkeling naar de eerste kolom’. We zullen zien dat ontwikkeling naar een andere kolom of een rij ook kan. Later zullen we een andere methode, ‘vegen’, zien om de determinant uit te rekenen.

### Mathematica

Invoer:

$$\text{Det}[\{\{1, 2, 3\}, \{-1, 0, 1\}, \{2, 3, 5\}\}]$$

Uitvoer:

$$2$$

Invoer:

$$\text{Inverse}[\{\{1, 2, 3\}, \{-1, 0, 1\}, \{2, 3, 5\}\}]$$

Uitvoer:

$$\left\{ \left\{ -\frac{3}{2}, -\frac{1}{2}, 1 \right\}, \left\{ \frac{7}{2}, -\frac{1}{2}, -2 \right\}, \left\{ -\frac{3}{2}, \frac{1}{2}, 1 \right\} \right\}$$

Invoer:

$$\text{TraditionalForm}[\%]$$

Uitvoer:

$$\begin{pmatrix} -\frac{3}{2} & -\frac{1}{2} & 1 \\ \frac{7}{2} & -\frac{1}{2} & -2 \\ -\frac{3}{2} & \frac{1}{2} & 1 \end{pmatrix}$$

### Mathematica

Invoer:

```
m = {{1, 2, 3}, {-1, 0, 1}, {2, 3, 5}};
LinearSolve[m, {2, 2, 4}]
```

Uitvoer:

$$\{0, -2, 2\}$$

Dit is equivalent met invoer:

```
Solve[{x + 2y + 3z == 2, -x + z == 2, 2x + 3y + 5z == 4}, {x, y, z}]
```

Uitvoer:

$$\{\{x \rightarrow 0, y \rightarrow -2, z \rightarrow 2\}\}$$

### Eigenschappen van de determinant

- De determinant verandert van teken als twee kolommen (of twee rijen) worden verwisseld, bijvoorbeeld

$$\det \begin{bmatrix} 1 & 2 & 4 \\ 3 & 8 & 1 \\ 0 & -1 & 7 \end{bmatrix} = -\det \begin{bmatrix} 3 & 8 & 1 \\ 1 & 2 & 4 \\ 0 & -1 & 7 \end{bmatrix}$$

Gevolg: ontwikkelen naar een andere kolom dan de eerste kan ook.

- De determinant verandert niet als de matrix wordt gespiegeld, bijvoorbeeld

$$\det \begin{bmatrix} 1 & 2 & 4 \\ 3 & 8 & 1 \\ 0 & -1 & 7 \end{bmatrix} = \det \begin{bmatrix} 1 & 3 & 0 \\ 2 & 8 & -1 \\ 4 & 1 & 7 \end{bmatrix}$$

Gevolg: ontwikkelen naar een rij in plaats van een kolom kan ook.

- De determinant wordt met een factor  $\alpha$  vermenigvuldigd als een kolom dat wordt, bijvoorbeeld

$$\det \begin{bmatrix} 1 & 2 & 4 \\ 3 & 8 & 1 \\ 0 & -1 & 7 \end{bmatrix} = 3 \det \begin{bmatrix} \frac{1}{3} & 2 & 4 \\ 1 & 8 & 1 \\ 0 & -1 & 7 \end{bmatrix}$$

**Eigenschappen van de determinant**

- De determinantfunctie is multiplicatief:  $\det(AB) = (\det A)(\det B)$
- $\det I = 1$ , en als  $A^{-1}$  bestaat, geldt dus  $\det(A^{-1}) = 1/\det A$
- Wordt een kolom van de matrix gesplitst als som van twee nieuwe kolommen, dan is de oorspronkelijke determinant de som van de zo ontstane nieuwe determinanten, bijvoorbeeld

$$\det \begin{bmatrix} 1 & 2 & 4 \\ 3 & 8 & 1 \\ 0 & -1 & 7 \end{bmatrix} = \det \begin{bmatrix} 1 & 1 & 4 \\ 3 & 5 & 1 \\ 0 & 4 & 7 \end{bmatrix} + \det \begin{bmatrix} 1 & 1 & 4 \\ 3 & 3 & 1 \\ 0 & -5 & 7 \end{bmatrix}$$

Wegens de spiegeleigenschap geldt hetzelfde voor rijen.

- De determinant is 0 als en alleen als de kolommen van de matrix afhankelijk zijn
- $\det A = 0 \iff \exists \vec{v} \mid \vec{v} \neq \vec{0} \bullet A\vec{v} = \vec{0}$
- De waarde van de determinant verandert niet als bij een kolom een veelvoud van een andere kolom wordt opgeteld ('vegen'), bijv.

$$\det \begin{bmatrix} 1 & 2 & 4 \\ 3 & 8 & 1 \\ 0 & -1 & 7 \end{bmatrix} = \det \begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & -11 \\ 0 & -1 & 7 \end{bmatrix}$$

**Bovendriehoeksmatrices**

Een matrix  $[a_{i,j}]_{i,j=1}^{n,n}$  heet een bovendriehoeksmatrix als

$$\forall i, j \mid 1 \leq j < i \leq n \bullet a_{i,j} = 0$$

Met volledige inductie naar  $n$  kunnen we bewijzen: als  $A = [a_{i,j}]_{i,j=1}^{n,n}$  een bovendriehoeksmatrix is, geldt

$$\det A = \prod_{i=1}^n a_{i,i}$$

(dus de determinant is het product van de termen op de diagonaal). Elke matrix kan door vegen in een bovendriehoeksmatrix worden omgezet.

**Bovendriehoeksmatrices**

Voorbeeld:

$$\begin{aligned} & \det \begin{bmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \\ 2 & 3 & 5 \end{bmatrix} \\ = & \{ \text{vegen met eerste rij} \} \\ & \det \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 4 \\ 0 & -1 & -1 \end{bmatrix} \end{aligned}$$

$$\begin{aligned}
&= \text{\{vegen met tweede rij\}} \\
&\det \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix} \\
&= \frac{\text{\{bovendriehoeksmatrix\}}}{2}
\end{aligned}$$

### Luma

Gekleurde bitmaps, voor televisie en computermonitoren, worden in eerste instantie uitgedrukt door per beeldpunt de kleurintensiteit in de componenten rood, groen en blauw uit te drukken. (Rood, groen en blauw zijn de kleuren van de afzonderlijke monitorelementen en ook de afzonderlijke kleuren die ons oog rechtstreeks kan zien. Andere kleuren ontstaan door menging.)

Voor gecompriemde afbeeldingen (JPEG, HDTV) wordt gebruik gemaakt van een andere kleurcodering: we definiëren bijvoorbeeld

$$\begin{aligned}
Y &= 0.299R + 0.587G + 0.114B \\
Cb &= B - Y \\
Cr &= R - Y
\end{aligned}$$

De reden is dat voor de indruk van scherpste vrijwel alleen de  $Y$ -component (*luma* genaamd) verantwoordelijk is. Daarom kan in de  $Cb$ - en  $Cr$ -componenten ongestraft het aantal pixels worden gereduceerd (downsampling).

### Luma



In matrixvorm kunnen we schrijven

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.299 & -0.587 & 0.886 \\ 0.701 & -0.587 & -0.114 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

Er geldt

$$\begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.299 & -0.587 & 0.886 \\ 0.701 & -0.587 & -0.114 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & -0.194 & -0.509 \\ 1 & 1 & 0 \end{bmatrix}$$

dus

$$R = Y + Cr$$

$$G = -0.194Cb - 0.509Cr$$

$$B = Y + Cb$$

## 9.4 Lineaire afbeeldingen

### Lineaire afbeeldingen

#### Definitie

Een *lineaire afbeelding*  $\sigma$  van  $\mathbb{R}^n$  naar  $\mathbb{R}^m$  is een afbeelding die voldoet aan

$$\sigma(\vec{x} + \vec{y}) = \sigma(\vec{x}) + \sigma(\vec{y})$$

$$\sigma(\alpha\vec{x}) = \alpha\sigma(\vec{x})$$

voor  $\vec{x}, \vec{y} \in \mathbb{R}^n$  en  $\alpha \in \mathbb{R}$ .

Voorbeelden van lineaire afbeeldingen van en naar  $\mathbb{R}^2$ :

- Spiegeling in een lijn door de oorsprong
- Rotatie om de oorsprong
- Vermenigvuldiging vanuit de oorsprong
- Projectie op een lijn door de oorsprong

### Lineaire afbeeldingen en matrices

Merk op dat voor een  $(m \times n)$ -matrix  $A$  de afbeelding  $\sigma$  van  $\mathbb{R}^n$  naar  $\mathbb{R}^m$ , gedefinieerd door  $\sigma(\vec{x}) = A\vec{x}$ , een lineaire afbeelding is. We laten zien dat *elke* lineaire afbeelding van deze vorm is.

Zij  $\sigma : \mathbb{R}^n \rightarrow \mathbb{R}^m$  een lineaire afbeelding. Beschouw

$$\vec{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n$$

Dit kunnen we ook schrijven als

$$\vec{x} = \sum_{j=1}^n x_j \vec{e}_j$$

waar  $\vec{e}_1, \dots, \vec{e}_n$  de standaardbasis voor  $\mathbb{R}^n$  is (dus  $\vec{e}_j = [[i = j]]_{i=1}^n$ ).

## Lineaire afbeeldingen en matrices

$$\begin{aligned}
 & \sigma(\vec{x}) \\
 = & \{ \vec{e}_1, \dots, \vec{e}_n \text{ standaardbasis voor } \mathbb{R}^n \} \\
 & \sigma(\sum_{j=1}^n x_j \vec{e}_j) \\
 = & \{ \text{lineariteit van } \sigma \} \\
 & \sum_{j=1}^n x_j \sigma(\vec{e}_j) \\
 = & \{ \vec{f}_1, \dots, \vec{f}_m \text{ standaardbasis voor } \mathbb{R}^m \} \\
 & \sum_{j=1}^n x_j \sum_{i=1}^m (\vec{f}_i \cdot \sigma(\vec{e}_j)) \vec{f}_i \\
 = & \{ \text{definieer } a_{i,j} = \vec{f}_i \cdot \sigma(\vec{e}_j) \} \\
 & \sum_{j=1}^n x_j \sum_{i=1}^m a_{i,j} \vec{f}_i \\
 = & \{ \text{verwisseling sommatievolgorde} \} \\
 & \sum_{i=1}^m (\sum_{j=1}^n a_{i,j} x_j) \vec{f}_i \\
 = & \{ \text{matrixvermenigvuldiging, waar } A = [a_{i,j}]_{i,j=1,1}^{m,n} \} \\
 & A\vec{x}
 \end{aligned}$$

Conclusie: alle lineaire afbeeldingen ontstaan door vermenigvuldiging met een matrix (naming de matrix waarvan  $\sigma(\vec{e}_1), \dots, \sigma(\vec{e}_n)$  de kolommen zijn.)

## 9.5 Eigenwaarden

### Eigenwaarden

Bestaat bij een  $(n \times n)$ -matrix  $A$  een getal  $\alpha$  en een vector  $\vec{v} \neq \vec{0}$  zó dat  $A\vec{v} = \alpha\vec{v}$ , dan heet  $\alpha$  een *eigenwaarde* en  $\vec{v}$  een *eigenvector* van  $A$ .

Als we een basis van  $\mathbb{R}^n$  kunnen vinden die geheel uit eigenvectoren bestaat, dan heeft  $A$  uitgedrukt in coördinaten ten opzichte van deze basis de gedaante van een *diagonaalmatrix*.

$$\begin{aligned}
 & \alpha \text{ is een eigenwaarde van } A \\
 \Leftrightarrow & \{ \text{definitie van eigenwaarde} \} \\
 & \exists \vec{v} \mid \vec{v} \neq \vec{0} \bullet A\vec{v} = \alpha\vec{v} \\
 \Leftrightarrow & \{ \text{optelling van matrices; } I \text{ de eenheidsmatrix} \} \\
 & \exists \vec{v} \mid \vec{v} \neq \vec{0} \bullet (A - \alpha I)\vec{v} = \vec{0} \\
 \Leftrightarrow & \{ \text{eigenschap determinant} \} \\
 & \det(A - \alpha I) = 0
 \end{aligned}$$

Het linkerlid van de vergelijking  $\det(A - \alpha I) = 0$  is een polynoom van de graad  $n$  in  $\alpha$ . Dit heet het *karakteristieke polynoom* van de matrix.

## 10 Binomiaalcoëfficiënten

### 10.1 Definitie

#### Combinatorische definitie

Voor niet-negatieve gehele getallen  $k$  en  $n$  definiëren we  $\binom{n}{k}$  als het aantal deelverzamelingen van  $k$  elementen uit een verzameling van  $n$  elementen. Uitspraak: ‘ $n$  boven  $k$ ’.

Voorbeeld: de verzameling  $\{1, 2, 3, 4\}$  heeft als deelverzamelingen met 2 elementen

$$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$$

dus  $\binom{4}{2} = 6$ .

Het aantal *rijen* van  $k$  verschillende elementen uit een verzameling met  $n$  elementen is

$$n(n-1)\dots(n-k+1) = n^{\underline{k}}$$

Elke deelverzameling met  $k$  elementen is op  $k!$  manieren als zo’n rij te schrijven. Conclusie:

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!}$$

### Generalisatie

Voor willekeurige reële  $r$  en gehele  $k$  definiëren we

$$\binom{r}{k} = \begin{cases} \frac{r^{\underline{k}}}{k!} & \text{als } k \geq 0 \\ 0 & \text{als } k < 0 \end{cases}$$

Merk op:

- Voor  $r \in \mathbb{N}_0$  (hier en verder is  $\mathbb{N}_0$  de verzameling van niet-negatieve gehele getallen) stemt dit met de combinatorische definitie overeen.
- $\binom{r}{k}$  is een polynoom in  $r$  van graad  $k$ .

### De driehoek van Pascal

Table 155 Pascal’s triangle.

$n$	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$	$\binom{n}{8}$	$\binom{n}{9}$	$\binom{n}{10}$
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

De blanco posities hebben de waarde 0 omdat  $n^{\underline{k}}$  daar een factor 0 bevat.

## 10.2 Identiteiten

### Verband met de faculteit

Voor  $k, n \in \mathbb{N}_0$  met  $k \leq n$  geldt

$$\begin{aligned}
 & \binom{n}{k} \\
 = & \left\{ \text{definitie van } \binom{n}{k}, \text{ gebruik } k \geq 0 \right\} \\
 & \frac{n^k}{k!} \\
 = & \left\{ \text{definitie van } n^k, \text{ gebruik } k \geq 0 \right\} \\
 & \frac{1}{k!} \prod_{j=0}^{k-1} (n-j) \\
 = & \left\{ \text{domeinsplitsing, gebruik } n \in \mathbb{N}_0 \text{ en } k \leq n \right\} \\
 & \frac{\prod_{j=0}^{n-1} (n-j)}{k! \prod_{j=k}^{n-1} (n-j)} \\
 = & \left\{ \text{dummytransformatie } j \leftarrow n-1 \right\} \\
 & \frac{\prod_{l=1}^n l}{k! \prod_{l=1}^{n-k} l} \\
 = & \left\{ \text{definitie van faculteit} \right\} \\
 & \frac{n!}{k!(n-k)!}
 \end{aligned}$$

### Symmetrie

Voor  $n \in \mathbb{N}_0, k \in \mathbb{Z}$  geldt

$$\binom{n}{k} = \binom{n}{n-k}$$

Als  $0 \leq k \leq n$ , zijn beide leden volgens de vorige identiteit immers gelijk aan

$$\frac{n!}{k!(n-k)!}$$

Als  $k < 0$ , is het linkerlid gelijk aan 0 wegens de definitie van  $\binom{n}{k}$ , en het rechterlid is gelijk aan 0 omdat in  $n^{\overline{n-k}}$  dan een factor 0 voorkomt. Als  $k > n$ , zijn beide leden 0 op grond van verwisselde argumentatie.

Deze identiteit verklaart waarom de rijen in de driehoek van Pascal symmetrisch zijn.

Waarschuwing: de identiteit geldt niet als  $n < 0$ , bijvoorbeeld  $\binom{-1}{2} = 1$  maar  $\binom{-1}{-3} = 0$ .

### Absorptie

Onder aanname van  $k > 0$  geldt

$$\begin{aligned}
 & k \binom{r}{k} \\
 = & \left\{ \text{definitie bin.co., gebruik } k \geq 0 \right\} \\
 & k \frac{r^k}{k!} \\
 = & \left\{ \text{recurrente betrekking voor } k!, \text{ gebruik } k > 0 \right\} \\
 & \frac{1}{(k-1)!} r^k \\
 = & \left\{ \text{definitie van } r^k \right\} \\
 & \frac{1}{(k-1)!} \prod_{j=0}^{k-1} (r-j) \\
 = & \left\{ \text{splits factor met } j=0 \text{ af, gebruik } k > 0 \right\}
 \end{aligned}$$

$$\begin{aligned}
 & \frac{1}{(k-1)!} r \prod_{j=1}^{k-1} (r-j) \\
 = & \quad \{ \text{dummytransformatie } j \leftarrow l+1 \} \\
 & \frac{1}{(k-1)!} r \prod_{l=0}^{k-2} (r-1-l) \\
 = & \quad \{ \text{definitie van } (r-1)^{\underline{k-1}} \} \\
 & \frac{1}{(k-1)!} r (r-1)^{\underline{k-1}} \\
 = & \quad \{ \text{definitie bin.co., gebruik } k-1 \geq 0 \} \\
 & r \binom{r-1}{k-1}
 \end{aligned}$$

### Absorptie

We hebben de identiteit

$$k \binom{r}{k} = r \binom{r-1}{k-1}$$

afgeleid voor  $k > 0$ . Maar als  $k \leq 0$ , geldt deze ook omdat dan beide leden 0 zijn.

Een analoge identiteit die de onderste index gelijk houdt, is

$$(r-k) \binom{r}{k} = r \binom{r-1}{k}$$

### Het polynoomargument

Voor  $r \in \mathbb{N}_0$  met  $r \geq 1$  is

$$\begin{aligned}
 & (r-k) \binom{r}{k} \\
 = & \quad \{ \text{symmetrie, gebruik } r \in \mathbb{N}_0 \} \\
 & (r-k) \binom{r}{r-k} \\
 = & \quad \{ \text{absorptie, met } k \leftarrow r-k \} \\
 & r \binom{r-1}{r-k-1} \\
 = & \quad \{ \text{symmetrie, gebruik } r-1 \in \mathbb{N}_0 \} \\
 & r \binom{r-1}{k}
 \end{aligned}$$

We hebben de identiteit nu afgeleid voor gehele positieve  $r$ . Maar beide leden van de gelijkheid zijn polynomen van graad  $k+1$  in  $r$ , dus het verschil is een polynoom van graad  $\leq k+1$  in  $r$  dat oneindig veel nulpunten heeft (alle positieve gehele waarden van  $r$ ). Zo'n polynoom moet identiek 0 zijn (hoofdstelling van de algebra).

Deze redenering zullen we onder de naam 'het polynoomargument' vaker gebruiken.

### De optelformule

In de driehoek van Pascal is elk getal de som van het getal links erboven en recht erboven. Dit volgt uit de *optelformule*

$$\binom{r}{k} = \binom{r-1}{k} + \binom{r-1}{k-1}$$

die ook voor negatieve  $k$  en niet-gehele  $r$  geldt.

Bewijs: voor  $r \neq 0$  geldt

$$\begin{aligned}
& \binom{r-1}{k} + \binom{r-1}{k-1} \\
= & \quad \{\text{absorptie, gebruik } r \neq 0\} \\
& \frac{r-k}{r} \binom{r}{k} + \frac{k}{r} \binom{r}{k} \\
= & \quad \{\text{rekenen}\} \\
& \binom{r}{k}
\end{aligned}$$

en dan geldt de formule voor alle  $r$  wegens het polynoomargument.

### Sommatie

De optelformule is een recurrente betrekking voor de rijen van de driehoek van Pascal. We kunnen deze gebruiken om formules met inductie te bewijzen. Voorbeeld:

$$\sum_{k=0}^n \binom{k}{m} = \binom{n+1}{m+1} \quad \text{voor } m, n \in \mathbb{N}_0$$

Inductie naar  $n$ . Basis:  $\binom{0}{m} = \binom{1}{m+1} = [m=0]$ . Stap: voor  $n \geq 1$  is

$$\begin{aligned}
& \sum_{k=0}^n \binom{k}{m} \\
= & \quad \{\text{splits af } k = n, \text{ gebruik } n \geq 0\} \\
& \sum_{k=0}^{n-1} \binom{k}{m} + \binom{n}{m} \\
= & \quad \{\text{inductiehypothese}\} \\
& \binom{n}{m+1} + \binom{n}{m} \\
= & \quad \{\text{optelformule}\} \\
& \binom{n+1}{m+1}
\end{aligned}$$

$$\text{Analoog: } \sum_{k=0}^n \binom{r+k}{k} = \binom{r+n+1}{n}$$

## 10.3 De binomiaalstelling

### De binomiaalstelling

De getallen in de driehoek van Pascal treden op als coëfficiënten in de expansie van  $(x+y)^n$ , als volgt:

$$\begin{aligned}
(x+y)^0 &= 1x^0y^0 \\
(x+y)^1 &= 1x^1y^0 + 1x^0y^1 \\
(x+y)^2 &= 1x^2y^0 + 2x^1y^1 + 1x^0y^2 \\
(x+y)^3 &= 1x^3y^0 + 3x^2y^1 + 3x^1y^2 + 1x^0y^3 \\
(x+y)^4 &= 1x^4y^0 + 4x^3y^1 + 6x^2y^2 + 4x^1y^3 + 1x^0y^4.
\end{aligned}$$

Combinatorisch gemakkelijk in te zien: aan een term  $x^k y^{n-k}$  wordt bijgedragen door bij het uitwerken van het product  $k$  maal de  $x$ -term en  $n-k$  maal de  $y$ -term te kiezen. Dit kan juist op  $\binom{n}{k}$  manieren.

**De binomiaalstelling**

**De binomiaalstelling**

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

(Wil dit ook gelden ingeval  $x = -y$ , dan moeten we definiëren  $0^0 = 1$ .) Bewijs met inductie naar  $n$ . Voor  $n = 0$  zijn beide leden 1, voor  $n > 0$  geldt

**De binomiaalstelling**

$$\begin{aligned} & (x + y)^n \\ = & \quad \{\text{rekenen}\} \\ & (x + y)(x + y)^{n-1} \\ = & \quad \{\text{inductiehypothese}\} \\ & (x + y) \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-1-k} \\ = & \quad \{\text{distributie}\} \\ & \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} y^{n-1-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\ = & \quad \{\text{dummytransformatie } k \leftarrow l - 1\} \\ & \sum_{l=1}^n \binom{n-1}{l-1} x^l y^{n-l} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\ = & \quad \{\text{splits af } l = n, k = 0; \text{ termsplitsing}\} \\ & x^n + y^n + \sum_{k=1}^{n-1} \left( \binom{n-1}{k-1} + \binom{n-1}{k} \right) x^k y^{n-k} \\ = & \quad \{\text{optelformule}\} \\ & x^n + y^n + \sum_{k=1}^{n-1} \binom{n}{k} x^k y^{n-k} \\ = & \quad \{\text{splits af } k = 0, k = n\} \\ & \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \end{aligned}$$

□

**Speciale gevallen**

Voor  $x = y = 1$  krijgen we:

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

(bijv.  $1 + 4 + 6 + 4 + 1 = 16$ ,  $1 + 5 + 10 + 10 + 5 + 1 = 32$ .)

Voor  $x = -1$ ,  $y = 1$  krijgen we:

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = [n = 0]$$

(bijv.  $1 - 4 + 6 - 4 + 1 = 0$ ,  $1 - 5 + 10 - 10 + 5 - 1 = 0$ .)

### Niet-natuurlijke exponent

Beschouw de functie

$$f(z) = (1 + z)^r$$

Deze is analytisch in  $z = 0$ , en met inductie kunnen we bewijzen dat

$$D^k f(z) = r^k (1 + z)^{r-k}$$

We hebben dus

$$\begin{aligned} f(z) &= \{ \text{Taylorreeks} \} \\ &= \sum_{k=0}^{\infty} \frac{D^k f(0)}{k!} z^k \\ &= \{ \text{formule voor } D^k f \} \\ &= \sum_{k=0}^{\infty} \frac{r^k}{k!} z^k \\ &= \{ \text{definitie bin.co.} \} \\ &= \sum_{k=0}^{\infty} \binom{r}{k} z^k \end{aligned}$$

### Niet-natuurlijke exponent

Het absolute quotiënt van opeenvolgende coëfficiënten is

$$\left| \frac{\binom{r}{k+1}}{\binom{r}{k}} \right| = \left| \frac{\frac{r^{k+1}}{(k+1)!}}{\frac{r^k}{k!}} \right| = \left| \frac{r-k}{k+1} \right| \rightarrow 1, \quad k \rightarrow \infty$$

dus de convergentiestraal is 1.

Dit geeft de meer algemene vorm van de binomiaalstelling:

$$(x + y)^r = \sum_k \binom{r}{k} x^k y^{r-k}$$

De som is eindig als  $r \in \mathbb{N}_0$  en een convergente reeks als  $|x| < |y|$ .

## 10.4 Producten

### Productformule

De formule

$$\binom{r}{m} \binom{m}{k} = \binom{r}{k} \binom{r-k}{m-k}$$

heeft de eigenschap dat die het dubbele voorkomen van  $m$  verwijdert, wat nuttig is ingeval  $m$  de sommatievariabele is. Bewijs: voor gehele  $r \geq m \geq k \geq 0$  geldt

$$\begin{aligned} &\binom{r}{m} \binom{m}{k} \\ &= \{ \text{verband met faculteit} \} \\ &= \frac{r!}{m!(r-m)!} \frac{m!}{k!(m-k)!} \\ &= \{ \text{vervang } m! \text{ in teller en noemer door } (r-k)! \} \\ &= \frac{r!}{k!(r-k)!} \frac{(r-k)!}{(m-k)!(r-m)!} \\ &= \{ \text{verband met faculteit} \} \\ &= \binom{r}{k} \binom{r-k}{m-k} \end{aligned}$$

Voor  $m < k$  of  $k < 0$  zijn beide leden 0. Dus de identiteit geldt voor willekeurige  $m$  en  $k$ , onder de voorwaarde dat  $m \geq k \geq 0 \Rightarrow r \in \mathbb{N}_0 \wedge r \geq m$ . Die laatste voorwaarde kan worden verwijderd met het polynoomargument.

### Sommen van producten

Table 169 Sums of products of binomial coefficients.	
$\sum_k \binom{r}{m+k} \binom{s}{n-k} = \binom{r+s}{m+n},$	integers $m, n.$ (5.22)
$\sum_k \binom{l}{m+k} \binom{s}{n+k} = \binom{l+s}{l-m+n},$	integer $l \geq 0,$ integers $m, n.$ (5.23)
$\sum_k \binom{l}{m+k} \binom{s+k}{n} (-1)^k = (-1)^{l+m} \binom{s-m}{n-l},$	integer $l \geq 0,$ integers $m, n.$ (5.24)
$\sum_{k \leq l} \binom{l-k}{m} \binom{s}{k-n} (-1)^k = (-1)^{l+m} \binom{s-m-1}{l-m-n},$	integers $l, m, n \geq 0.$ (5.25)
$\sum_{0 \leq k \leq l} \binom{l-k}{m} \binom{q+k}{n} = \binom{l+q+1}{m+n+1},$	integers $l, m \geq 0,$ integers $n \geq q \geq 0.$ (5.26)

Niet zinvol deze van buiten te leren!

### Quotiënten

$$\begin{aligned} & \sum_{k=0}^m \binom{m}{k} / \binom{n}{k} \\ = & \quad \{\text{productformule}\} \\ & \sum_{k=0}^m \binom{n-k}{m-k} / \binom{n}{m} \\ = & \quad \{\text{dummytransformatie } k \leftarrow m-l\} \\ & \sum_{l=0}^m \binom{n-m+l}{l} / \binom{n}{m} \\ = & \quad \{\text{sommatie-identiteit}\} \\ & \binom{(n-m)+m+1}{m} / \binom{n}{m} \\ = & \quad \{\text{rekenen}\} \\ & \binom{n+1}{m} / \binom{n}{m} \\ = & \quad \{\text{absorptie}\} \\ & \frac{n+1}{n+1-m} \end{aligned}$$

## 10.5 Newtonreeksen

### Newtonreeksen

Omdat  $\binom{x}{k}$  een polynoom van graad  $k$  is, is elk polynoom van graad  $d$  te schrijven in de vorm

$$f(x) = \sum_{k=0}^d c_k \binom{x}{k}$$

bijvoorbeeld

$$\begin{aligned}
 & x^2 + 2x + 3 \\
 = & \left\{ \binom{x}{2} = \frac{1}{2}x^2 - \frac{1}{2}x \right\} \\
 & 2\binom{x}{2} + 3x + 3 \\
 = & \left\{ \binom{x}{1} = x \right\} \\
 & 2\binom{x}{2} + 3\binom{x}{1} + 3 \\
 = & \left\{ \binom{x}{0} = 1 \right\} \\
 & 2\binom{x}{2} + 3\binom{x}{1} + 3\binom{x}{0}
 \end{aligned}$$

Een dergelijke ontwikkeling heet de *Newtonreeks* van  $f$ .

### Differenties

Er geldt

$$\Delta(\lambda x \bullet \binom{x}{k}) = \lambda x \bullet \binom{x}{k-1}$$

dus voor

$$f(x) = \sum_{k=0}^d c_k \binom{x}{k}$$

geldt

$$\Delta^n f(x) = \sum_{k=0}^d c_k \binom{x}{k-n}$$

In het bijzonder is

$$\Delta^n f(0) = \begin{cases} c_n & \text{als } n \leq d \\ 0 & \text{als } n > d \end{cases}$$

dus de Newtonreeks van  $f$  is te schrijven als

$$f(x) = \sum_{k=0}^d \Delta^k f(0) \binom{x}{k}$$

### Binomiaalcoëfficiënten in de informatica

In een boom is de *padlengte* de som, genomen over alle knopen, van hun afstand tot de wortel.

- In een binaire boom met  $N$  knopen is de padlengte gemiddeld

$$\frac{(N+1)4^N}{\binom{2N}{N}} - 3N - 1$$

- In een boom met  $N$  knopen is de padlengte gemiddeld

$$\frac{N}{2} \left( \frac{4^{N-1}}{\binom{2N-2}{N-1}} - 1 \right)$$

## Het verjaardagsprobleem

Bij de *hashtable*-datastructuur worden geheugenadressen toebedeeld door een versleuteling van de waarde die moet worden opgeslagen. We zijn erin geïnteresseerd hoe vaak dit tot een botsing leidt (twee verschillende waarden waaraan hetzelfde adres wordt toegekend).

Populaire versie van hetzelfde probleem: hoe groot is de kans dat twee mensen in een groep dezelfde verjaardag hebben?

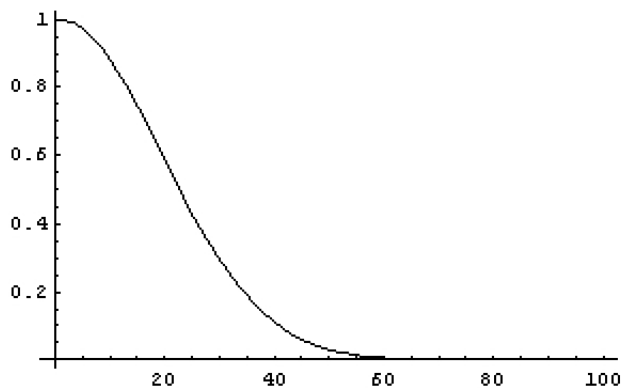
Beschouw een groep met  $N$  personen. De kans dat persoon 2 niet dezelfde verjaardag heeft als persoon 1 is  $1 - 1/m$ , met  $m = 365$ . De kans dat de verjaardag van persoon 3 verschilt van de andere twee is vervolgens  $1 - 2/m$ , enzovoort; in totaal is de kans dat alle  $N$  personen een verschillende verjaardag hebben

$$\prod_{k=1}^{N-1} \left(1 - \frac{k}{m}\right) = \frac{m^N}{m^N} = \frac{N!}{m^N} \binom{m}{N}$$

## Het verjaardagsprobleem

Mathematica:

```
In[4]:= Plot[Binomial[365, N] * N! / (365^N), {N, 0, 100}]
```



# 11 Voortbrengende functies

## 11.1 Repertoire

### Voortbrengende functies

Bij een gegeven rij  $\langle a_k \rangle_{k=0}^{\infty}$  kunnen we de bijbehorende *machtrees*

$$A(z) = \sum_{k=0}^{\infty} a_k z^k$$

beschouwen. De functie  $A$  is gedefinieerd op het convergentiegebied van de machtrees en kan een hulpmiddel zijn om het gedrag van de rij beter te begrijpen; we noemen  $A$  de *voortbrengende functie* van  $\langle a_k \rangle_{k=0}^{\infty}$ .

Voorbeeld: voor de voortbrengende functie  $A$  van de rij

$$\left\langle \frac{1}{k!} \right\rangle_{k=0}^{\infty}$$

geldt

$$A(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z$$

### Toepassing van de binomiaalstelling

Voor de voortbrengende functie  $A$  van de rij

$$\left\langle \binom{r}{k} \right\rangle_{k=0}^{\infty}$$

geldt

$$A(z) = \sum_{k=0}^{\infty} \binom{r}{k} z^k = (1+z)^r$$

volgens de binomiaalstelling.

### Negatie

De *negatieformule* voor binomiaalcoëfficiënten, die we in het volgende vaak gaan gebruiken, zegt

$$\binom{r}{k} = (-1)^k \binom{k-r-1}{k}$$

Bewijs: Voor  $k \geq 0$  geldt

$$\begin{aligned} & r^{\underline{k}} \\ = & \{ \text{definitie } r^{\underline{k}} \} \\ & \prod_{j=0}^{k-1} (r-j) \\ = & \{ \text{haal } k \text{ factoren } (-1) \text{ buiten het product} \} \\ & (-1)^k \prod_{j=0}^{k-1} (j-r) \\ = & \{ \text{dummytransformatie } j \leftarrow k-1-l \} \\ & (-1)^k \prod_{l=0}^{k-1} (k-r-1-l) \\ = & \{ \text{definitie } (k-r-1)^{\underline{k}} \} \\ & (-1)^k (k-r-1)^{\underline{k}} \end{aligned}$$

en voor  $k < 0$  zijn beide leden 0. □

### Exponent $-1$

Speciaal geval:  $r = -1$ . We krijgen

$$\begin{aligned}
 &= \frac{1}{1+z} \\
 &= \{ \text{binomiaalstelling} \} \\
 &= \sum_{k=0}^{\infty} \binom{-1}{k} z^k \\
 &= \{ \text{negatie, met } r = -1 \} \\
 &= \sum_{k=0}^{\infty} (-1)^k \binom{k}{k} z^k \\
 &= \{ \binom{k}{k} = 1 \} \\
 &= \sum_{k=0}^{\infty} (-1)^k z^k
 \end{aligned}$$

dus de voortbrengende functie van  $\langle (-1)^k \rangle_{k=0}^{\infty}$  is  $\lambda z \bullet \frac{1}{1+z}$ .

Vervangen van  $z$  door  $-z$  geeft: de voortbrengende functie van  $\langle 1 \rangle_{k=0}^{\infty}$  is  $\lambda z \bullet \frac{1}{1-z}$ .

### Omgekeerde binomiaalstelling

Volgens de binomiaalstelling is

$$\sum_{k=0}^{\infty} \binom{n}{k} z^k = (1+z)^n$$

Maar hoe zit het met

$$\sum_{k=0}^{\infty} \binom{k}{n} z^k ?$$

### Omgekeerde binomiaalstelling

$$\begin{aligned}
 &= \sum_{k=0}^{\infty} \binom{k}{n} z^k \\
 &= \{ \binom{k}{n} = 0 \text{ als } k < n \} \\
 &= \sum_{k=n}^{\infty} \binom{k}{n} z^k \\
 &= \{ \text{dummytransformatie } k \leftarrow l + n \} \\
 &= \sum_{l=0}^{\infty} \binom{l+n}{n} z^{l+n} \\
 &= \{ \text{distributie van } z^n \} \\
 &= z^n \sum_{l=0}^{\infty} \binom{l+n}{n} z^l \\
 &= \{ \text{symmetriestelling} \} \\
 &= z^n \sum_{l=0}^{\infty} \binom{l+n}{l} z^l \\
 &= \{ \text{negatie, met } r = l + n \} \\
 &= z^n \sum_{l=0}^{\infty} (-1)^l \binom{-n-1}{l} z^l \\
 &= \{ \text{binomiaalstelling} \} \\
 &= \frac{z^n}{(1-z)^{n+1}}
 \end{aligned}$$

dus de voortbrengende functie van  $\langle \binom{k}{n} \rangle_{k=0}^{\infty}$  is  $\lambda z \bullet \frac{z^n}{(1-z)^{n+1}}$ .

### Toepassing van de Newtonreeks

Gevraagd: de voortbrengende functie van  $\langle k^2 \rangle_{k=0}^{\infty}$ . Er geldt

$$\begin{aligned}
 & \sum_{k=0}^{\infty} k^2 z^k \\
 = & \left\{ \binom{k}{2} = \frac{1}{2}k^2 - \frac{1}{2}k \right\} \\
 & \sum_{k=0}^{\infty} \left( 2\binom{k}{2} + k \right) z^k \\
 = & \left\{ \binom{k}{1} = k \right\} \\
 & \sum_{k=0}^{\infty} \left( 2\binom{k}{2} + \binom{k}{1} \right) z^k \\
 = & \left\{ \text{termsplitsing} \right\} \\
 & 2 \sum_{k=0}^{\infty} \binom{k}{2} z^k + \sum_{k=0}^{\infty} \binom{k}{1} z^k \\
 = & \left\{ \text{omgekeerde binomiaalstelling} \right\} \\
 & 2 \frac{z^2}{(1-z)^3} + \frac{z}{(1-z)^2}
 \end{aligned}$$

## 11.2 Convolutie

### Convolutie

Als  $A$  de voortbrengende functie van  $\langle a_k \rangle_{k=0}^{\infty}$  is, en  $B$  die van  $\langle b_k \rangle_{k=0}^{\infty}$ , dan is  $A + B$  de voortbrengende functie van  $\langle a_k + b_k \rangle_{k=0}^{\infty}$  (gebruik termsplitsing). Maar hoe zit het met  $AB$ ?

$$\begin{aligned}
 & AB(z) \\
 = & \left\{ A \text{ en } B \text{ zijn voortbrengende functies} \right\} \\
 & \sum_{k=0}^{\infty} a_k z^k \sum_{l=0}^{\infty} b_l z^l \\
 = & \left\{ \text{dubbelsom} \right\} \\
 & \sum_{k,l} [k \geq 0][l \geq 0] a_k b_l z^{k+l} \\
 = & \left\{ \text{dummytransformatie } l \leftarrow n - k \right\} \\
 & \sum_{k,n} [k \geq 0][n \geq k] a_k b_{n-k} z^n \\
 = & \left\{ \text{dubbelsom} \right\} \\
 & \sum_{n=0}^{\infty} \left( \sum_{k=0}^n a_k b_{n-k} \right) z^n
 \end{aligned}$$

dus  $AB$  is de voortbrengende functie van

$$\left\langle \sum_{k=0}^n a_k b_{n-k} \right\rangle_{n=0}^{\infty}$$

het convolutieproduct van  $\langle a_k \rangle_{k=0}^{\infty}$  en  $\langle b_k \rangle_{k=0}^{\infty}$ .

### Convolutie met constante term

Het convolutieproduct van  $\langle a_k \rangle_{k=0}^{\infty}$  en  $\langle 1 \rangle_{k=0}^{\infty}$  is

$$\left\langle \sum_{k=0}^n a_k \right\rangle_{n=0}^{\infty}$$

de rij van *partiële sommen* van  $\sum_{n=0}^{\infty} a_n$ .

Als  $A$  de voortbrengende functie van  $\langle a_k \rangle_{k=0}^{\infty}$  is, dan is de voortbrengende functie van  $\langle \sum_{k=0}^n a_k \rangle_{n=0}^{\infty}$  gelijk aan

$$\lambda z \bullet \frac{A(z)}{1-z}$$

**Vandermonde's convolutie**

Beschouw het convolutieproduct van

$$\left\langle \binom{r}{k} \right\rangle_{k=0}^{\infty} \text{ en } \left\langle \binom{s}{k} \right\rangle_{k=0}^{\infty}$$

Dit is de rij

$$\left\langle \sum_{k=0}^n \binom{r}{k} \binom{s}{n-k} \right\rangle_{n=0}^{\infty}$$

De voortbrengende functie is

$$(1+z)^r(1+z)^s$$

Maar dat is gelijk aan  $(1+z)^{r+s}$ . Volgens de binomiaalstelling is dus

$$\sum_{k=0}^n \binom{r}{k} \binom{s}{n-k} = \binom{r+s}{n}$$

(Combinatorische interpretatie: kies  $n$  mensen uit een gezelschap van  $r$  mannen en  $s$  vrouwen.)

**Derangementen**

Een derangement van  $[1..n]$  is een permutatie die geen enkel element op zijn plaats laat. Zij  $n_i$  (' $n$  subfaculteit') het aantal derangementen van  $[1..n]$ . Dan zijn er  $\binom{n}{k}(n-k)_i$  permutaties van  $[1..n]$  die precies  $k$  elementen op zijn plaats laten, dus

$$n! = \sum_{k=0}^n \binom{n}{k} (n-k)_i$$

ofwel

$$1 = \sum_{k=0}^n \frac{1}{k!} \frac{(n-k)_i}{(n-k)!}$$

Het rechterlid is de  $n$ -de term in het convolutieproduct van  $\left\langle \frac{1}{k!} \right\rangle_{k=0}^{\infty}$  en  $\left\langle \frac{k_i}{k!} \right\rangle_{k=0}^{\infty}$ . Conclusie:

$$\frac{1}{1-z} = e^z \sum_{k=0}^{\infty} \frac{k_i}{k!} z^k$$

**Derangementen**

$$\begin{aligned} & \sum_{n=0}^{\infty} \frac{n_i}{n!} z^n \\ = & \left\{ \text{voorgaande conclusie, vermenigvuldig beide leden met } e^{-z} \right\} \\ & \frac{e^{-z}}{1-z} \\ = & \left\{ \text{voortbrengende functies} \right\} \\ & \sum_{k=0}^{\infty} \frac{(-1)^k z^k}{k!} \sum_{l=0}^{\infty} z^l \\ = & \left\{ \text{convolutie} \right\} \\ & \sum_{n=0}^{\infty} \left( \sum_{k=0}^n \frac{(-1)^k}{k!} \right) z^n \end{aligned}$$

Conclusie:

$$n_j = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$$

### Derangementen

Wat is de kans dat een willekeurige permutatie een derangement is?

$$\begin{aligned} & \frac{n_j}{n!} \\ &= \{ \text{voorgaande conclusie} \} \\ & \sum_{k=0}^n \frac{(-1)^k}{k!} \\ & \rightarrow \{ \text{voor } n \rightarrow \infty \} \\ &= \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \\ &= \{ \text{Taylorreeks van } \exp \} \\ & e^{-1} \\ & \approx \{ \} \\ & 0.367\dots \end{aligned}$$

### Derangementen

Mathematica: invoer

$$N[\text{Sum}[(-1)^k/k!, k, 0, 50], 20]$$

of invoer

$$\ll \text{DiscreteMath`CombinatorialFunctions`}$$

$$N[\text{Subfactorial}[50]/50!, 20]$$

of invoer

$$N[\text{Exp}[-1], 20]$$

geven alle als uitvoer

$$0.36787944117144232160$$

## 11.3 Recurrente betrekkingen

### Recurrente betrekkingen

We geven een voorbeeld om te laten zien hoe recurrente betrekkingen (ook) met behulp van voortbrengende functies kunnen worden opgelost. Beschouw de recurrente betrekking

$$f_n = f_{n-1} + f_{n-2} \text{ voor } n \geq 2$$

(zoals Fibonacci), met  $f_0$  en  $f_1$  gegeven constanten. Zij  $F$  de voortbrengende functie van de rij  $\langle f_n \rangle_{n=0}^{\infty}$ . Dan

$$\begin{aligned}
 & F(z) \\
 &= \{ \text{voortbrengende functie} \} \\
 &= \sum_{n=0}^{\infty} f_n z^n \\
 &= \{ \text{splits af } n=0 \text{ en } n=1 \} \\
 &= f_0 + f_1 z + \sum_{n=2}^{\infty} f_n z^n \\
 &= \{ \text{recurrente betrekking} \} \\
 &= f_0 + f_1 z + \sum_{n=2}^{\infty} (f_{n-1} + f_{n-2}) z^n \\
 &= \{ \text{termsplitsing; dummytransformatie } n \leftarrow k+1 \text{ en } n \leftarrow l+2 \} \\
 &= f_0 + f_1 z + z \sum_{k=1}^{\infty} f_k z^k + z^2 \sum_{l=0}^{\infty} f_l z^l \\
 &= \{ \text{voortbrengende functie} \} \\
 &= f_0 + f_1 z + z(F(z) - f_0) + z^2 F(z)
 \end{aligned}$$

### Recurrente betrekkingen

$$\begin{aligned}
 & F(z) = f_0 + f_1 z + z(F(z) - f_0) + z^2 F(z) \\
 & \Leftrightarrow \{ \text{rekenen} \} \\
 & (1 - z - z^2)F(z) = f_0 + (f_1 - f_0)z \\
 & \Leftrightarrow \{ \text{rekenen} \} \\
 & F(z) = \frac{f_0 + (f_1 - f_0)z}{1 - z - z^2}
 \end{aligned}$$

Er geldt  $1 - z - z^2 = -(z - \alpha)(z - \beta)$ , waar  $\alpha = (-1 + \sqrt{5})/2$  en  $\beta = (-1 - \sqrt{5})/2$ . Volgens de theorie van breuksplitsing kunnen we dan A en B vinden met

$$\frac{f_0 + (f_1 - f_0)z}{1 - z - z^2} = \frac{A}{z - \alpha} + \frac{B}{z - \beta}$$

### Berekening van de coëfficiënten

$$\begin{aligned}
 & \forall z \mid z \neq \alpha \wedge z \neq \beta \bullet \frac{f_0 + (f_1 - f_0)z}{1 - z - z^2} = \frac{A}{z - \alpha} + \frac{B}{z - \beta} \\
 & \Leftrightarrow \{ \text{vermenigvuldig beide leden met } (z - \alpha)(z - \beta); \text{ polynoomargument} \} \\
 & \forall z \bullet -(f_0 + (f_1 - f_0)z) = A(z - \beta) + B(z - \alpha) \\
 & \Rightarrow \{ \text{vul in } z = \alpha, z = \beta \} \\
 & A = \frac{-(f_0 + (f_1 - f_0)\alpha)}{\alpha - \beta} \wedge B = \frac{-(f_0 + (f_1 - f_0)\beta)}{\beta - \alpha}
 \end{aligned}$$

### Substitutie in de voortbrengende functie

$$\begin{aligned}
 & F(z) \\
 &= \{ \text{eerder afgeleid} \} \\
 &= \frac{A}{z - \alpha} + \frac{B}{z - \beta} \\
 &= \{ \text{deel factor } \alpha \text{ resp. } \beta \text{ uit teller en noemer} \} \\
 &= \frac{A/\alpha}{1 - z/\alpha} - \frac{B/\beta}{1 - z/\beta} \\
 &= \{ \text{repertoire} \} \\
 &= -\frac{A}{\alpha} \sum_{n=0}^{\infty} \alpha^{-n} z^n - \frac{B}{\beta} \sum_{n=0}^{\infty} \beta^{-n} z^n \\
 &= \{ \text{termsplitsing} \} \\
 &= \sum_{n=0}^{\infty} \left( -\frac{A}{\alpha} \alpha^{-n} - \frac{B}{\beta} \beta^{-n} \right) z^n
 \end{aligned}$$

Omdat  $F$  de voortbrengende functie van  $\langle f_n \rangle_{n=0}^\infty$  is, volgt

$$f_n = -\frac{A}{\alpha} \alpha^{-n} - \frac{B}{\beta} \beta^{-n}$$

## 11.4 Goedhaakse expressies

### Goedhaakse expressies

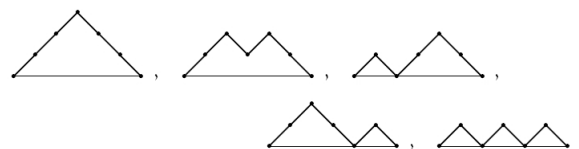
Beschouw een expressie in  $n + 1$  variabelen

$$x_0 \otimes x_1 \otimes \cdots \otimes x_n$$

We willen weten op hoeveel verschillende manieren hierin door het zetten van haakjes een evaluatievolgorde kan worden aangegeven. Voor  $n = 3$  zijn er bijvoorbeeld 5 mogelijkheden, namelijk

$$x_0 \otimes (x_1 \otimes (x_2 \otimes x_3)), \quad x_0 \otimes ((x_1 \otimes x_2) \otimes x_3), \quad (x_0 \otimes x_1) \otimes (x_2 \otimes x_3) \\ (x_0 \otimes (x_1 \otimes x_2)) \otimes x_3, \quad ((x_0 \otimes x_1) \otimes x_2) \otimes x_3$$

Grafisch kunnen we dit als volgt weergeven: zet een extra stel haakjes rond de hele formule en representeer elke  $\otimes$  door / en elke  $\otimes$  door \. Er ontstaan dan zgn. *Klammergebirge*:



### De recurrente betrekking

Zij  $n > 0$ . In dat geval bevat de expressie ten minste één  $\otimes$ . Beschouw het voorkomen van  $\otimes$  op het hoogste niveau, buiten alle haakjes. Laat die voorkomen tussen  $x_k$  en  $x_{k+1}$ . In dat geval is het voorgaande stuk een goedhaakse indeling van  $x_0 \otimes x_1 \otimes \cdots \otimes x_k$ , en het eropvolgende stuk een goedhaakse indeling van  $x_{k+1} \otimes x_{k+2} \otimes \cdots \otimes x_n$ .

Dus, als voor elke  $n$  met  $C_n$  het aantal goedhaakse indelingen van  $x_0 \otimes x_1 \otimes \cdots \otimes x_n$  wordt aangegeven, geldt

$$C_n = \sum_{k=0}^{n-1} C_k C_{n-1-k} \quad \text{voor } n > 0$$

Voor  $n = 0$  geeft deze formule niet de goede waarde, want  $C_0 = 1$ . In het algemeen geldt dus

$$C_n = \sum_{k=0}^{n-1} C_k C_{n-1-k} + [n = 0]$$

**De voortbrengende functie**

Zij  $C$  de voortbrengende functie van  $\langle C_n \rangle_{n=0}^\infty$ . Dan

$$\begin{aligned}
 & C(z) \\
 = & \{ \text{voortbrengende functie} \} \\
 & \sum_{n=0}^{\infty} C_n z^n \\
 = & \{ \text{splits af } n = 0 \} \\
 & C_0 + \sum_{n=1}^{\infty} C_n z^n \\
 = & \{ \text{recurrente betrekking} \} \\
 & 1 + \sum_{n=1}^{\infty} \left( \sum_{k=0}^{n-1} C_k C_{n-1-k} \right) z^n \\
 = & \{ \text{dummytransformatie } n \leftarrow n + 1 ; \text{ factor } z \text{ buiten de sommatie halen} \} \\
 & 1 + z \sum_{l=0}^{\infty} \left( \sum_{k=0}^l C_k C_{l-k} \right) z^l \\
 = & \{ \text{convolutie} \} \\
 & 1 + z(C(z))^2
 \end{aligned}$$

**De voortbrengende functie**

$C$  voldoet dus aan de vergelijking

$$C(z) = 1 + z(C(z))^2$$

Beschouwd als kwadratische vergelijking in de onbekende  $C(z)$  levert dit de oplossingen

$$C(z) = \frac{1 \pm \sqrt{1 - 4z}}{2z}$$

De oplossing met  $+$  heeft limiet  $\infty$  voor  $z \rightarrow 0$  en correspondeert dus niet met een machtreeks. Conclusie:

$$C(z) = \frac{1 - \sqrt{1 - 4z}}{2z}$$

**Berekening van de coëfficiënten**

$$\begin{aligned}
 & \sqrt{1 - 4z} \\
 = & \{ \text{binomiaalstelling} \} \\
 & \sum_{k=0}^{\infty} \binom{1/2}{k} (-4z)^k \\
 = & \{ \text{splits af } k = 0 \} \\
 & 1 + \sum_{k=1}^{\infty} \binom{1/2}{k} (-4z)^k \\
 = & \{ \text{factor } (-4z) \text{ buiten som halen} \} \\
 & 1 - 4z \sum_{k=1}^{\infty} \binom{1/2}{k} (-4z)^{k-1}
 \end{aligned}$$

dus

$$\begin{aligned}
 & \frac{1 - \sqrt{1 - 4z}}{2z} \\
 = & \{ \text{voorgaande resultaat} \} \\
 & 2 \sum_{k=1}^{\infty} \binom{1/2}{k} (-4z)^{k-1} \\
 = & \{ \text{dummytransformatie } k \leftarrow n + 1 \} \\
 & 2 \sum_{n=0}^{\infty} \binom{1/2}{n+1} (-4)^n z^n
 \end{aligned}$$

dus

$$C_n = 2 \binom{1/2}{n+1} (-4)^n$$

### Alternatieve formule

$$\begin{aligned} & 2 \binom{1/2}{n+1} (-4)^n \\ = & \{ \text{definitie bin.co.} \} \\ & \frac{2}{(n+1)!} \prod_{j=0}^n \left(\frac{1}{2} - j\right) (-4)^n \\ = & \{ \text{splits af } j = 0; \text{ distribueer } n \text{ factoren } -2 \} \\ & \frac{1}{(n+1)!} \prod_{j=1}^n (2j - 1) 2^n \\ = & \{ (2n)! = \prod_{j=1}^n (2j - 1) \prod_{k=1}^n (2k) \} \\ & \frac{1}{(n+1)!} \frac{(2n)!}{n!} \\ = & \{ (n+1)! = (n+1)n! \} \\ & \frac{1}{n+1} \frac{(2n)!}{(n!)^2} \\ = & \{ \text{eigenschap bin.co.} \} \\ & \frac{1}{n+1} \binom{2n}{n} \end{aligned}$$

dus er geldt ook

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

## 12 Kansrekening

### 12.1 Kansruimten

#### Kansmaat

Een *experiment* is een handeling of serie handelingen met een of meer mogelijke resultaten (*uitkomsten* genoemd). De *uitkomstenruimte*, die we steeds zullen aangeven met  $\Omega$ , is de verzameling van alle mogelijke uitkomsten van het experiment. We bestuderen hier alleen het geval van een eindige verzameling  $\Omega$ .

Voorbeeld: het experiment bestaat uit gooien met twee dobbelstenen. De uitkomstenruimte is dan

$$\{1 \wr 1, 1 \wr 2, \dots, 1 \wr 6, 2 \wr 1, 2 \wr 2, \dots, 6 \wr 6\}$$

(waarbij we de uitkomsten  $1 \wr 2$  en  $2 \wr 1$  als verschillend beschouwen). Er zijn dus  $6^2 = 36$  mogelijke uitkomsten.

Een *kansmaat* of *kansverdeling* op een uitkomstenruimte  $\Omega$  is een afbeelding  $\text{Pr} : \Omega \rightarrow [0..1]$  die voldoet aan

$$\sum_{\omega \in \Omega} \text{Pr}(\omega) = 1$$

Het paar  $(\Omega, \text{Pr})$  heet een *kansruimte*.

**Kansmaat**

De *uniforme* kansverdeling op een uitkomstenruimte  $\Omega$  is de kansverdeling waarbij elke uitkomst even waarschijnlijk is, dus waarvoor geldt

$$\forall \omega \in \Omega \bullet \Pr(\omega) = 1/\#\Omega$$

Het voorbeeld met de twee dobbelstenen is een uniforme kansverdeling.

Bij gegeven kansruimte  $(\Omega, \Pr)$  kunnen we ook de *verdubbelde* kansruimte beschouwen. De uitkomsten zijn hier paren van uitkomsten uit  $\Omega$ , en de kansmaat daarop is gedefinieerd door

$$\Pr(\omega_1, \omega_2) = \Pr(\omega_1) \cdot \Pr(\omega_2)$$

Het voorbeeld met de twee dobbelstenen is op die manier ontstaan uit de kansruimte van een enkele dobbelsteen. Op deze manier kunnen herhaalde experimenten *die elkaar niet beïnvloeden* worden gemodelleerd. De verdubbelde kansruimte heeft een uniforme verdeling als dat voor de oorspronkelijke geldt.

**Gebeurtenissen**

Een *gebeurtenis* is een deelverzameling van  $\Omega$ .

Voorbeeld: in het experiment met de twee dobbelstenen is een gebeurtenis

$$\{1 \wr 1, 2 \wr 2, 3 \wr 3, 4 \wr 4, 5 \wr 5, 6 \wr 6\}$$

(het gooien van 'dubbel').

Voor elke gebeurtenis  $A$  definiëren we de *kans* op  $A$  als

$$\Pr(A) = \sum_{\omega \in A} \Pr(\omega)$$

In het bijzonder  $\Pr(\{\omega\}) = \Pr(\omega)$ . De eenpuntsverzamelingen  $\{\omega\}$  noemen we *elementaire gebeurtenissen*.

Bij zuivere dobbelstenen is de kans op elke elementaire gebeurtenis in bovenstaand voorbeeld  $\frac{1}{36}$ , dus de kans op 'dubbel' is  $6 \cdot \frac{1}{36} = \frac{1}{6}$ .

**Stochasten**

Een *stochast* ('random variable') is een afbeelding van de uitkomstenruimte naar de reële getallen. We noteren stochasten steeds met hoofdletters en de waarden die ze aannemen met dezelfde kleine letters. In het bijzonder noteren we

$$\Pr(X = x) = \Pr(\{\omega \mid X(\omega) = x\}) = \sum_{\omega \in \Omega} [X(\omega) = x] \Pr(\omega)$$

In het voorbeeld met twee dobbelstenen beschouwen we de stochast  $S$  die het totaal aantal gegooide ogen telt, dus bijvoorbeeld  $S(6 \wr 3) = 9$ . Dan

$$\Pr(S = 5) = \Pr(1 \wr 4) + \Pr(2 \wr 3) + \Pr(3 \wr 2) + \Pr(4 \wr 1)$$

Bij zuivere dobbelstenen is de kans op  $S = 5$  dus  $4 \cdot \frac{1}{36} = \frac{1}{9}$ .

**Onafhankelijke stochasten**

Stochasten  $X$  en  $Y$  heten *onafhankelijk* als

$$\forall x, y \bullet \Pr(X = x \wedge Y = y) = \Pr(X = x) \cdot \Pr(Y = y)$$

Voorbeeld: als  $S_1$  de gegooidde waarde van de eerste dobbelsteen en  $S_2$  die van de tweede is, zijn  $S_1$  en  $S_2$  onafhankelijk. Als  $S = S_1 + S_2$  en  $P = S_1 \cdot S_2$ , zijn  $S$  en  $P$  niet onafhankelijk, want bijvoorbeeld

$$\begin{aligned} \Pr(S = 2 \wedge P = 1) &= \Pr(1 \wedge 1) = \frac{1}{36} \\ \Pr(S = 2) \cdot \Pr(P = 1) &= (\Pr(1 \wedge 1))^2 = \frac{1}{36^2} = \frac{1}{1296} \end{aligned}$$

**Verwachtingswaarde**

De *verwachtingswaarde* van een stochast is gedefinieerd als

$$EX = \sum_{\omega \in \Omega} X(\omega) \Pr(\omega)$$

Alternatieve schrijfwijze:

$$\begin{aligned} & \sum_{\omega \in \Omega} X(\omega) \Pr(\omega) \\ &= \text{\{eenpuntsdomein\}} \\ & \sum_{\omega \in \Omega} \Pr(\omega) \sum_{x \in \mathbb{R}} x [X(\omega) = x] \\ &= \text{\{dubbelsom\}} \\ & \sum_{x \in \mathbb{R}} x \sum_{\omega \in \Omega} [X(\omega) = x] \Pr(\omega) \\ &= \text{\{notatie Pr(X = x)\}} \\ & \sum_{x \in \mathbb{R}} x \Pr(X = x) \end{aligned}$$

dus

$$EX = \sum_{x \in \mathbb{R}} x \Pr(X = x)$$

met ander woorden:  $EX$  is de gemiddelde waarde van  $X$ .

**Som en product van stochasten**

Uit de definitie van verwachtingswaarde volgt direct dat voor stochasten  $X$  en  $Y$  geldt

$$E(X + Y) = EX + EY$$

en, voor constante  $\alpha$ ,

$$E(\alpha X) = \alpha \cdot EX$$

(Analoog aan college 9 drukken we dit samen uit door  $E$  een *lineaire afbeelding* te noemen.)

Voor *onafhankelijke* stochasten geldt bovendien

$$E(XY) = EX \cdot EY$$

**Som en product van stochasten**

$$\begin{aligned}
& E(XY) \\
&= \quad \{\text{definitie verwachtingswaarde}\} \\
&\quad \sum_{\omega \in \Omega} X(\omega)Y(\omega)\Pr(\omega) \\
&= \quad \{\text{eenpuntsdomein}\} \\
&\quad \sum_{\omega \in \Omega} \Pr(\omega) \sum_{x \in \mathbb{R}} \sum_{y \in \mathbb{R}} xy[X(\omega) = x \wedge Y(\omega) = y] \\
&= \quad \{\text{dubbelsom}\} \\
&\quad \sum_{x \in \mathbb{R}} \sum_{y \in \mathbb{R}} xy \sum_{\omega \in \Omega} [X(\omega) = x \wedge Y(\omega) = y]\Pr(\omega) \\
&= \quad \{\text{notatie}\} \\
&\quad \sum_{x \in \mathbb{R}} \sum_{y \in \mathbb{R}} xy \cdot \Pr(X = x \wedge Y = y) \\
&= \quad \{\text{als } X \text{ en } Y \text{ onafhankelijk zijn}\} \\
&\quad \sum_{x \in \mathbb{R}} \sum_{y \in \mathbb{R}} xy \cdot \Pr(X = x)\Pr(Y = y) \\
&= \quad \{\text{dubbelsom}\} \\
&\quad \sum_{x \in \mathbb{R}} x \cdot \Pr(X = x) \cdot \sum_{y \in \mathbb{R}} y \cdot \Pr(Y = y) \\
&= \quad \{\text{verwachtingswaarde is gemiddelde waarde}\} \\
&\quad EX \cdot EY
\end{aligned}$$

**12.2 Variantie****Variantie**

Hoeveel verschillen de echte waarden die een stochast aanneemt van de verwachtingswaarde? De *variantie* van een stochast  $X$  is gedefinieerd als

$$VX = E((X - EX)^2)$$

Voorbeeld: is het beter twee loten in dezelfde loterij te kopen of twee loten in verschillende loterijen? Stel er zijn 100 loten per loterij en de prijs is  $P$ . Laat  $X_1$  en  $X_2$  de verwachtingswaarde van de gewonnen prijs op het eerste resp. tweede lot zijn, en  $X = X_1 + X_2$  de verwachtingswaarde voor het totaal gewonnen bedrag; dan is

$$\begin{aligned}
& EX \\
&= \quad \{X = X_1 + X_2; E \text{ is additief}\} \\
&\quad EX_1 + EX_2 \\
&= \quad \{\text{gegevens loterijen}\} \\
&\quad (0.99 \cdot 0 + 0.01 \cdot P) + (0.99 \cdot 0 + 0.01 \cdot P) \\
&= \quad \{\text{rekenen}\} \\
&\quad 0.02P
\end{aligned}$$

ongeacht de gevolgde strategie.

**Variantie**

Maar de kansmaat is in beide gevallen niet dezelfde! In geval van twee loterijen hebben we

Uitkomst	$0 \searrow 0$	$0 \searrow P$	$P \searrow 0$	$P \searrow P$
Kans	0.9801	0.0099	0.0099	0.0001
$X$	0	$P$	$P$	$2P$
$(X - 0.02P)^2$	$0.0004P^2$	$0.9604P^2$	$0.9604P^2$	$3.9204P^2$

dus

$$\begin{aligned}
 & VX \\
 = & \quad \{\text{definitie } V; EX = 0.02P\} \\
 & E((X - 0.02P)^2) \\
 = & \quad \{\text{verwachtingswaarde als gemiddelde waarde}\} \\
 & 0.9801 \cdot 0.0004P^2 + 0.0198 \cdot 0.9604P^2 + 0.0001 \cdot 3.9204P^2 \\
 = & \quad \{\text{rekenen}\} \\
 & (0.00039204 + 0.01901592 + 0.00039204)P^2 \\
 = & \quad \{\text{rekenen}\} \\
 & 0.0198P^2
 \end{aligned}$$

(Opmerkelijk weinig decimalen – zullen we later verklaren.)

### Variantie

In het geval dat de twee loten in dezelfde loterij worden gekocht:

Uitkomst	0	P
Kans	0.98	0.02
X	0	P
$(X - 0.02P)^2$	$0.0004P^2$	$0.9604P^2$

dus

$$\begin{aligned}
 & VX \\
 = & \quad \{\text{definitie } V; EX = 0.02P\} \\
 & E((X - 0.02P)^2) \\
 = & \quad \{\text{verwachtingswaarde als gemiddelde waarde}\} \\
 & 0.98 \cdot 0.0004P^2 + 0.02 \cdot 0.9604P^2 \\
 = & \quad \{\text{rekenen}\} \\
 & (0.000392 + 0.019208)P^2 \\
 = & \quad \{\text{rekenen}\} \\
 & 0.0196P^2
 \end{aligned}$$

Deze kansmaat heeft een iets kleinere variantie, dus minder risico.

### Standaarddeviatie

Veelal geven we de voorkeur aan een maat voor de afwijking van het gemiddelde die dezelfde dimensie heeft als de stochast zelf. De *standaarddeviatie* is gedefinieerd als

$$\sigma = \sqrt{VX}$$

In het voorgaande voorbeeld is bij twee loterijen

$$\sigma = \sqrt{0.0198P^2} \approx 0.140712473P$$

en bij één loterij

$$\sigma = \sqrt{0.0196P^2} = 0.14P$$

dus de mate van extra risico in het geval van twee loterijen is te waarderen op  $0.000712473P$  (bij een prijs van 1 miljoen euro is dit dus € 712.47).

**Eenvoudiger formule voor de variantie**

$$\begin{aligned}
& VX \\
= & \quad \{\text{definitie}\} \\
& E((X - EX)^2) \\
= & \quad \{\text{rekenen}\} \\
& E(X^2 - 2X \cdot EX + (EX)^2) \\
= & \quad \{E \text{ is lineair; } EX \text{ is constant}\} \\
& E(X^2) - 2EX \cdot EX + (EX)^2 \\
= & \quad \{\text{rekenen}\} \\
& E(X^2) - (EX)^2
\end{aligned}$$

dus

$$VX = E(X^2) - (EX)^2$$

(‘De variantie is het gemiddelde van het kwadraat min het kwadraat van het gemiddelde.’)

Dit verklaart de ‘ronde’ uitkomsten van de loterijberekening.

**Additiviteit van variantie**

Voor onafhankelijke stochasten  $X$  en  $Y$  geldt

$$\begin{aligned}
& V(X + Y) \\
= & \quad \{ VX = E(X^2) - (EX)^2 \} \\
& E((X + Y)^2) - (E(X + Y))^2 \\
= & \quad \{\text{rekenen; lineariteit van } E\} \\
& E(X^2) + 2E(XY) + E(Y^2) - ((EX)^2 + 2EX \cdot EY + (EY)^2) \\
= & \quad \{ E(XY) = EX \cdot EY \text{ want } X \text{ en } Y \text{ onafhankelijk} \} \\
& E(X^2) - (EX)^2 + E(Y^2) - (EY)^2 \\
= & \quad \{ VX = E(X^2) - (EX)^2 \} \\
& VX + VY
\end{aligned}$$

dus

$$V(X + Y) = VX + VY$$

voor *onafhankelijke* stochasten.

(Merk op dat  $V$  niet lineair is:  $V(\alpha \cdot X) = \alpha^2 \cdot VX$ .)

**Ongelijkheid van Chebyshev**

Het is wel duidelijk dat de variantie iets zegt over de te verwachten afwijking van het gemiddelde, maar wat precies? Het precieze antwoord is de *ongelijkheid van Chebyshev* (heeft niets te maken met de ongelijkheid van Chebyshev uit college 3):

$$\Pr((X - EX)^2 \geq \alpha) \leq \frac{VX}{\alpha}$$

want

$$\begin{aligned}
& VX \\
&= \{ \text{definitie } V \text{ en } E \} \\
&= \sum_{\omega \in \Omega} (X(\omega) - EX)^2 \Pr(\omega) \\
&\geq \{ \text{zij } A = \{ \omega \in \Omega \mid (X(\omega) - EX)^2 \geq \alpha \} \} \\
&= \sum_{\omega \in A} (X(\omega) - EX)^2 \Pr(\omega) \\
&\geq \{ \text{definitie van } A \} \\
&= \sum_{\omega \in A} \alpha \cdot \Pr(\omega) \\
&= \{ \text{eigenschap } \Pr \} \\
&= \alpha \cdot \Pr(A) \\
&= \{ \text{definitie van } A \} \\
&= \alpha \cdot \Pr((X - EX)^2 \geq \alpha)
\end{aligned}$$

### Ongelijkheid van Chebyshev

Zij  $\mu$  de verwachtingswaarde en  $\sigma$  de standaarddeviatie van  $X$ , en kies in de ongelijkheid van Chebyshev in het bijzonder  $\alpha = c^2 VX$ . De ongelijkheid wordt dan

$$\Pr(|X - \mu| \geq c\sigma) \leq \frac{1}{c^2}$$

Met  $c = 2$  vinden we:  $X$  ligt binnen 2 standaarddeviaties van  $\mu$  met kans 75%. Met  $c = 10$  vinden we:  $X$  ligt binnen 10 standaarddeviaties van  $\mu$  met kans 99%.

De schattingen die uit de ongelijkheid van Chebyshev volgen, blijken in de praktijk overigens veel te ruim te zijn.

### Wet van de grote aantallen

Zij  $X$  een stochast op  $\Omega$  met verwachtingswaarde  $\mu$  en standaarddeviatie  $\sigma$ . Beschouw de kansruimte  $(\Omega^n, \Pr)$  met

$$\Pr(\omega_1, \omega_2, \dots, \omega_n) = \Pr(\omega_1)\Pr(\omega_2) \cdots \Pr(\omega_n)$$

en daarop de stochast

$$\bar{X} = \frac{1}{n}(X(\omega_1) + X(\omega_2) + \cdots + X(\omega_n))$$

(de gemiddelde uitkomst van  $n$  experimenten). Dan heeft  $\bar{X}$  verwachtingswaarde  $\mu$ .

### Wet van de grote aantallen

$$\begin{aligned}
& V\bar{X} \\
&= \{ \text{definitie van } \bar{X} \} \\
&= V\left(\frac{1}{n} \sum_{j=1}^n X(\omega_j)\right) \\
&= \{ \text{termen zijn onafhankelijke stochasten} \} \\
&= \frac{1}{n^2} \sum_{j=1}^n V(X(\omega_j)) \\
&= \{ V(X(\omega_j)) = \sigma^2 \} \\
&= \frac{\sigma^2}{n}
\end{aligned}$$

Conclusie: de standaarddeviatie van  $\bar{X}$  is  $\frac{\sigma}{\sqrt{n}}$ . Deze waarde kan onbeperkt klein worden gemaakt door  $n$  maar groot genoeg te kiezen. (Dit staat bekend als de ‘zwakke wet van de grote aantallen’; voor de ‘sterke’ variant zie het college Statistiek.)

### Schatten van onbekende kansen

Stel dat we de kansmaat niet kennen, maar wel een experiment kunnen herhalen. Als  $n$  onafhankelijk experimenten respectievelijk uitkomst  $X_1, X_2, \dots, X_n$  hebben, kunnen we als schatting voor  $EX$  uitgaan van

$$\hat{E}X = \frac{1}{n} \sum_{j=1}^n X_j$$

immers,

$$\begin{aligned} & E(\hat{E}X) \\ &= \{ \text{definitie } \hat{E} \} \\ & E\left(\frac{1}{n} \sum_{j=1}^n X_j\right) \\ &= \{ \text{lineariteit van } E \} \\ & \frac{1}{n} \sum_{j=1}^n EX_j \\ &= \{ EX_j = EX \} \\ & EX \end{aligned}$$

### Schatten van onbekende kansen

En als schatting voor  $VX$  kunnen we uitgaan van

$$\hat{V}X = \frac{1}{n-1} \sum_{j=1}^n X_j^2 - \frac{1}{n(n-1)} \left( \sum_{j=1}^n X_j \right)^2$$

(de factoren  $n - 1$  in de noemer zijn verrassend!)

### Schatten van onbekende kansen

$$\begin{aligned} & E(\hat{V}X) \\ &= \{ \text{definitie van } \hat{V}; \text{ schrijf kwadraat van som als dubbelsom} \} \\ & E\left(\frac{1}{n-1} \left( \sum_{j=1}^n X_j^2 - \frac{1}{n} \sum_{j=1}^n \sum_{k=1}^n X_j X_k \right)\right) \\ &= \{ \text{lineariteit van } E \} \\ & \frac{1}{n-1} \left( \sum_{j=1}^n E(X_j^2) - \frac{1}{n} \sum_{j=1}^n \sum_{k=1}^n E(X_j X_k) \right) \\ &= \{ \text{onafhankelijkheid van } X_j \text{ en } X_k \} \\ & \frac{1}{n-1} \left( \sum_{j=1}^n E(X_j^2) - \frac{1}{n} \sum_{j=1}^n \sum_{k=1}^n ([j \neq k] EX_j \cdot EX_k + [j = k] E(X_j^2)) \right) \\ &= \{ EX_j = EX \} \\ & \frac{1}{n-1} \left( \sum_{j=1}^n E(X^2) - \frac{1}{n} \sum_{j=1}^n \sum_{k=1}^n ([j \neq k] EX \cdot EX + [j = k] E(X^2)) \right) \\ &= \{ \text{constante term} \} \\ & \frac{1}{n-1} \left( nE(X^2) - \frac{1}{n}(n(n-1)(EX)^2 + nE(X^2)) \right) \end{aligned}$$

$$\begin{aligned}
&= \text{\{rekenen\}} \\
&E(X^2) - (EX)^2 \\
&= \text{\{eigenschap V\}} \\
&VX
\end{aligned}$$

### 12.3 Kansvoortbrengende functies

#### Kansvoortbrengende functies

Zij  $X$  een stochast die alleen niet-negatieve gehele waarden aanneemt. De kansvoortbrengende functie (pgf) van  $X$  is gedefinieerd als

$$G_X(z) = \sum_{k=0}^{\infty} \Pr(X = k)z^k$$

Alternatieve formuleringen:

$$\begin{aligned}
G_X(z) &= \sum_{\omega \in \Omega} \Pr(\omega)z^{X(\omega)} \\
G_X(z) &= E(z^X)
\end{aligned}$$

waaruit volgt

$$\begin{aligned}
&G_X(1) \\
&= \text{\{alternatieve formulering van definitie } G_X \text{\}} \\
&\sum_{\omega \in \Omega} \Pr(\omega) \\
&= \text{\{Pr is een kansmaat\}} \\
&1
\end{aligned}$$

#### Verwachtingswaarde

$$\begin{aligned}
&EX \\
&= \text{\{verwachtingswaarde als gemiddelde\}} \\
&\sum_{k=0}^{\infty} \Pr(X = k) \cdot k \\
&= \text{\{ } k = (\lambda z \bullet kz^{k-1})(1) \text{ voor } k \geq 1 \text{\}} \\
&(\lambda z \bullet \sum_{k=1}^{\infty} \Pr(X = k) \cdot kz^{k-1})(1) \\
&= \text{\{differentiëren van machtreeks, zie college 4\}} \\
&D(\lambda z \bullet \sum_{k=0}^{\infty} \Pr(X = k)z^k)(1) \\
&= \text{\{definitie van } G_X \text{\}} \\
&DG_X(1)
\end{aligned}$$

dus

$$EX = G'_X(1)$$

**Variantie**

$$\begin{aligned}
& E(X^2) \\
&= \{ \text{verwachtingswaarde als gemiddelde} \} \\
& \sum_{k=0}^{\infty} \Pr(X = k) \cdot k^2 \\
&= \{ k^2 = (\lambda z \bullet k(k-1)z^{k-2} + kz^{k-1})(1) \text{ voor } k \geq 2 \} \\
& 1 + (\lambda z \bullet \sum_{k=2}^{\infty} \Pr(X = k)(k(k-1)z^{k-2} + kz^{k-1}))(1) \\
&= \{ \text{differentiëren van machtreeks} \} \\
& (D^2 + D) (\lambda z \bullet \sum_{k=0}^{\infty} \Pr(X = k)z^k) (1) \\
&= \{ \text{definitie van } G_X \} \\
& (D^2 + D)G_X(1)
\end{aligned}$$

dus

$$VX = G_X''(1) + G_X'(1) - G_X'(1)^2$$

**Additiviteit**

Als  $X$  en  $Y$  onafhankelijke stochasten zijn die alleen niet-negatieve gehele waarden aannemen, geldt

$$\begin{aligned}
& G_{X+Y}(z) \\
&= \{ \text{definitie pgf} \} \\
& \sum_{n=0}^{\infty} \Pr(X + Y = n)z^n \\
&= \{ X, Y \text{ niet-negatief en geheel} \} \\
& \sum_{n=0}^{\infty} \sum_{k=0}^n \Pr(X = k \wedge Y = n - k)z^n \\
&= \{ X, Y \text{ onafhankelijk} \} \\
& \sum_{n=0}^{\infty} \sum_{k=0}^n \Pr(X = k)\Pr(Y = n - k)z^n \\
&= \{ \text{convolutie} \} \\
& (\sum_{k=0}^{\infty} \Pr(X = k)z^k) (\sum_{m=0}^{\infty} \Pr(Y = m)z^m) \\
&= \{ \text{definitie pgf} \} \\
& G_X(z) \cdot G_Y(z)
\end{aligned}$$

dus

$$G_{X+Y} = G_X G_Y$$

**13 Asymptotiek****13.1 Asymptotiek****Orden van grootte**

We willen uitspraken doen over de groeisnelheid van functies van een natuurlijk argument  $n$  wanneer  $n$  zich in de richting van  $\infty$  beweegt. Notatie: voor functies  $f, g : \mathbb{N} \rightarrow \mathbb{R}$  definiëren we

$$f \prec g \iff \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$$

Voorbeeld:

$$(\lambda n \bullet n) \prec (\lambda n \bullet n^2)$$

Om het opschrijven van  $\lambda$ -expressies te vermijden, schrijven we in plaats van  $f \prec g$  ook wel  $f(n) \prec g(n)$ ,  $n \rightarrow \infty$ . Zo wordt het voorbeeld

$$n \prec n^2, \quad n \rightarrow \infty$$

Merk op dat  $n$  hierin een *gebonden variabele* is, wat door het bijschrift  $n \rightarrow \infty$  wordt duidelijk gemaakt. Dit weglaten, zoals het boek veelal doet, is formeel minder juist.

### Voorbeelden

- $n^\alpha \prec n^\beta$ ,  $n \rightarrow \infty \iff \alpha < \beta$
- $\ln n \prec n^\alpha$ ,  $n \rightarrow \infty \iff \alpha > 0$
- $n^\alpha \prec e^n$ ,  $n \rightarrow \infty$  voor alle  $\alpha$
- $\alpha^n \prec \beta^n$ ,  $n \rightarrow \infty \iff \alpha < \beta$
- $\alpha^n \prec n^n$ ,  $n \rightarrow \infty$  voor alle  $\alpha$

Numerieke vergelijking: voor  $n = 1000$  is

$$\begin{aligned} \ln n &\approx 6.9 \\ n^2 &= 10^6 \\ e^n &\approx 2.0 \cdot 10^{434} \\ n^n &= 10^{3000} \end{aligned}$$

(Merk op dat  $10^{434}$  nanoseconden  $\approx 10^{417}$  jaar, dus een algoritme met exponentiële complexiteit is niet praktisch. De huidige leeftijd van het universum wordt geschat op  $10^{10}$  jaar.)

### Asymptotische gelijkheid

Notatie: voor functies  $f, g : \mathbb{N} \rightarrow \mathbb{R}$  definiëren we

$$f \sim g \iff \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$$

In plaats van  $f \sim g$  schrijven we weer vaak  $f(n) \sim g(n)$ ,  $n \rightarrow \infty$ . Voorbeeld:

$$\sum_{k=1}^n k \sim \frac{1}{2}n^2, \quad n \rightarrow \infty$$

In de vorige hoofdstukken schreven we in zo'n geval ' $f(n) \approx g(n)$ ' voor grote  $n$ '. De relatie  $\sim$  maakt de begrippen 'ongeveer' en 'groot' in dit verband exact.

**Asymptotische begrenstheid**

Notatie: voor functies  $f, g : \mathbb{N} \rightarrow \mathbb{R}$  definiëren we

$$f \ll g \iff \exists C, N \bullet \forall n \mid n > N \bullet |f(n)| \leq C|g(n)|$$

$$f \asymp g \iff f \ll g \wedge g \ll f$$

In plaats van  $f \asymp g$  schrijven we ook weer  $f(n) \asymp g(n)$ ,  $n \rightarrow \infty$ . Deze relatie drukt uit dat  $f$  en  $g$  op den duur ten hoogste een constante factor verschillen. Er geldt

$$f \sim g \Rightarrow f \asymp g$$

maar de omgekeerde implicatie geldt niet. Voorbeeld:

$$2 + \sin n \asymp 1, \quad n \rightarrow \infty$$

want de functie in het linkerlid is begrensd door 1 en 3; maar het linkerlid heeft geen limiet!

**Het O-symbool van Landau-Bachmann**

We hebben eerder (in college 3) bewezen dat

$$\ln n + \frac{1}{n} \leq H_n \leq \ln n + 1$$

Vaak vatten we het essentiële hieruit samen door te zeggen dat

$$H_n = \ln n + O(1), \quad n \rightarrow \infty$$

Hierin stelt  $O(1)$  een begrensde term voor waarin we verder niet geïnteresseerd zijn. Meer algemeen kunnen we in een formule  $O(f(n))$  schrijven; dit stelt een *onbepaalde* expressie  $g(n)$  voor die voldoet aan

$$g(n) \ll f(n), \quad n \rightarrow \infty$$

Vergelijk het gebruik van onbepaalde constanten in de integraalrekening.

Voorbeeld:  $n^m = n^m + O(n^{m-1})$ ,  $n \rightarrow \infty$ .

**Het O-symbool van Landau-Bachmann**

Uit

$$n = O(n^3), \quad n \rightarrow \infty$$

$$n^2 = O(n^3), \quad n \rightarrow \infty$$

kunnen we *niet* concluderen dat  $n = n^2$ . Het  $=$ -symbool in deze formules voldoet dan ook niet aan de normale wetten zoals symmetrie. Het zou beter geweest zijn een ander symbool te gebruiken zoals  $\sqsubseteq$ ; immers, het linkerlid is een *verfijning* van het onvolledig gespecificeerde rechterlid. Helaas wil de traditie anders.

Men gaat zelfs zo ver formules op te schrijven als

$$2n^2 + O(n) = O(n^2), \quad n \rightarrow \infty$$

De betekenis hiervan is: voor elke  $f$  die voldoet aan  $f(n) \ll n$ ,  $n \rightarrow \infty$  geldt

$$2n^2 + f(n) \ll n^2, \quad n \rightarrow \infty$$

**Verwante symbolen**

Waar  $O$  een bovengrens voor de groeiorde aangeeft, wordt  $\Omega$  gebruikt voor een ondergrens:  $\Omega(f(n))$  stelt een onbepaalde expressie  $g(n)$  voor die voldoet aan  $f(n) \ll g(n)$ ,  $n \rightarrow \infty$ . Gevolg:

$$f(n) = O(g(n)), n \rightarrow \infty \iff g(n) = \Omega(f(n)), n \rightarrow \infty$$

$\Theta(f(n))$  stelt een onbepaalde expressie  $g(n)$  voor die voldoet aan  $f(n) \asymp g(n)$ ,  $n \rightarrow \infty$ . Gevolg:

$$f(n) = \Theta(g(n)), n \rightarrow \infty \iff f(n) = O(g(n)), n \rightarrow \infty \\ \wedge f(n) = \Omega(g(n)), n \rightarrow \infty$$

Voorbeeld: sorteren van een rij getallen met Mergesort kost  $\Theta(n \log n)$  vergelijkingen.

Tenslotte:  $o(f(n))$  stelt een onbepaalde expressie  $g(n)$  voor die voldoet aan  $f(n) \prec g(n)$ ,  $n \rightarrow \infty$ . Gevolg:

$$f \sim g \iff f(n) = g(n) + o(g(n)), n \rightarrow \infty$$

**13.2 Reeksontwikkelingen****Afkappen van een convergente machtreeks**

Als een machtreeks

$$S(z) = \sum_{n=0}^{\infty} a_n z^n$$

absoluut convergeert voor enig complex getal  $z_0$ , is

$$|S(z)| \leq \sum_{n=0}^{\infty} |a_n z_0^n| \text{ voor alle } z \text{ met } |z| \leq |z_0|$$

waaruit volgt

$$S\left(\frac{1}{n}\right) = O(1), n \rightarrow \infty$$

en zelfs

$$S\left(\frac{1}{n}\right) = \sum_{k=0}^{m-1} \frac{a_k}{n^k} + O\left(\frac{1}{n^m}\right), n \rightarrow \infty$$

**Afkappen van een convergente machtreeks**

Voorbeelden:

$$\frac{n}{n-1} = 1 + \frac{1}{n} + \frac{1}{n^2} + \frac{1}{n^3} + O\left(\frac{1}{n^4}\right), n \rightarrow \infty$$

$$\ln\left(1 + \frac{1}{n}\right) = \frac{1}{n} - \frac{1}{2n^2} + \frac{1}{3n^3} + O\left(\frac{1}{n^4}\right), n \rightarrow \infty$$

$$\exp \frac{1}{n} = 1 + \frac{1}{n} + \frac{1}{2n^2} + \frac{1}{6n^3} + O\left(\frac{1}{n^4}\right), n \rightarrow \infty$$

**Andere reeksontwikkelingen**

De onderstaande ontwikkelingen zijn *niet* uit een convergente machtreeks ontstaan:

Table 452 Asymptotic approximations, valid as  $n \rightarrow \infty$  and  $z \rightarrow 0$ .

$$H_n = \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\left(\frac{1}{n^6}\right). \quad (9.28)$$

$$n! = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \left(1 + \frac{1}{12n} + \frac{1}{288n^2} - \frac{139}{51840n^3} + O\left(\frac{1}{n^4}\right)\right). \quad (9.29)$$

$$\pi(n) = \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + \frac{2!n}{(\ln n)^3} + \frac{3!n}{(\ln n)^4} + O\left(\frac{n}{(\log n)^5}\right). \quad (9.31)$$

Dat kan, omdat convergentie van zo'n reeks iets zegt over het gedrag van  $\sum_{k=1}^m \frac{a_k}{n^k}$  voor  $m \rightarrow \infty$  bij vaste  $n$ , terwijl we nu geïnteresseerd zijn in het gedrag van deze som voor  $n \rightarrow \infty$  bij vaste  $m$ .

**13.3 O-manipulatie**

**O-manipulatie**

Wetten als

$$f(n) = O(f(n)), \quad n \rightarrow \infty$$

$$O(f(n))O(g(n)) = O(f(n)g(n)), \quad n \rightarrow \infty$$

volgen onmiddellijk uit de definities. Interessanter is de volgende wet:

$$f \prec 1 \Rightarrow \ln(1 + O(f(n))) = O(f(n)), \quad n \rightarrow \infty$$

Immers, zij  $f \prec 1$  en  $g$  een willekeurige functie die voldoet aan  $g \ll f$ . Dit laatste houdt het bestaan van  $C$  en  $N$  in met

$$\forall n \mid n > N \bullet |g(n)| \leq C|f(n)|$$

Omdat  $f \prec 1$ , d.w.z.  $\lim_{n \rightarrow \infty} f(n) = 0$ , kunnen we  $N$  ook zo groot kiezen dat

$$\forall n \mid n > N \bullet C|f(n)| < \frac{1}{2}$$

**Logaritmwet**

De Taylorreeks van  $\ln(1 + g(n))$  is

$$\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} g(n)^k$$

Hierin is, voor  $n > N$  en alle  $k$ ,

$$\left| \frac{(-1)^{k+1}}{k} g(n)^k \right| < |g(n)| \frac{1}{2^{k-1}}$$

zodat de Taylorreeks convergeert naar  $\ln(1+g(n))$  en de som begrensd is door een constante maal  $|f(n)|$ . Hiermee is bewezen dat

$$\ln(1 + O(f(n))) = O(f(n)), \quad n \rightarrow \infty$$

### Exponentwet

Een tweede wet, met eenzelfde bewijs, is

$$f \ll 1 \Rightarrow \exp O(f(n)) = 1 + O(f(n)), \quad n \rightarrow \infty$$

Combinatie van de twee wetten geeft

$$f \prec 1 \wedge fg \ll 1 \Rightarrow (1 + O(f(n)))^{O(g(n))} = 1 + O(f(n)g(n)), \quad n \rightarrow \infty$$

immers, voor  $n \rightarrow \infty$ ,

$$\begin{aligned} & (1 + O(f(n)))^{O(g(n))} \\ = & \quad \{\text{definitie machtsverheffing}\} \\ & \exp(O(g(n)) \ln(1 + O(f(n)))) \\ = & \quad \{f \prec 1, \text{logaritmewet}\} \\ & \exp(O(g(n))O(f(n))) \\ = & \quad \{\text{elementaire O-manipulatie}\} \\ & \exp O(f(n)g(n)) \\ = & \quad \{fg \ll 1, \text{exponentwet}\} \\ & 1 + O(f(n)g(n)) \end{aligned}$$

### Mergesort

Bij de behandeling van Mergesort in college 2 hadden we voor het aantal vergelijkingen gevonden

$$M_n = nL_n - 2^{L_n} + 1$$

waarin  $L_n$  het kleinste getal  $i$  is waarvoor  $2^i \geq n$ . In onze huidige notatie is dus

$$L_n = \lceil \lg n \rceil = \lg n + O(1)$$

dus

$$\begin{aligned} & M_n \\ = & \quad \{\text{college 2}\} \\ & nL_n - 2^{L_n} + 1 \\ = & \quad \{L_n = \lg n + O(1)\} \\ & n(\lg n + O(1)) - 2^{\lg n + O(1)} + 1 \\ = & \quad \{\text{rekenen}\} \\ & n \cdot \lg n + n \cdot O(1) - n \cdot 2^{O(1)} + 1 \\ = & \quad \{\text{O-manipulatie}\} \\ & n \cdot \lg n + O(n) \end{aligned}$$

**Som van wortels**

In college 5 hebben we afgeleid

$$\sum_{k=0}^{n-1} \lfloor \sqrt{k} \rfloor = na - \frac{1}{3}a^3 - \frac{1}{2}a^2 - \frac{1}{6}a$$

waarin  $a = \lfloor \sqrt{n} \rfloor$ . Dus

$$\begin{aligned} & na - \frac{1}{3}a^3 - \frac{1}{2}a^2 - \frac{1}{6}a \\ = & \left\{ a = n^{1/2} + O(1) \right\} \\ & n^{3/2} - \frac{1}{3}(n^{1/2} + O(1))^3 - \frac{1}{2}(n^{1/2} + O(1))^2 - \frac{1}{6}(n^{1/2} + O(1)) \\ = & \left\{ O\text{-manipulatie} \right\} \\ & n^{3/2} - \frac{1}{3}(n^{3/2} + O(n)) - \frac{1}{2} \cdot O(n) - \frac{1}{6} \cdot O(n^{1/2}) \\ = & \left\{ O\text{-manipulatie} \right\} \\ & \frac{2}{3}n^{3/2} + O(n) \end{aligned}$$

**13.4 Bootstrapping**

**Het k-de priemgetal**

We gaan uit van de priemgetalstelling in de vorm

$$\pi(n) = \frac{n}{\ln n} + O\left(\frac{n}{(\ln n)^2}\right), \quad n \rightarrow \infty$$

Kies voor  $n$  in het bijzonder het  $k$ -de priemgetal. Dan is  $\pi(n) = k$ . In het bijzonder geldt

$$\frac{n}{\ln n} \sim k, \quad k \rightarrow \infty$$

dus  $n/\ln n = O(k)$  en

$$O\left(\frac{n}{(\ln n)^2}\right) = O\left(\frac{k}{\ln k}\right), \quad k \rightarrow \infty$$

Dit speciale geval van de priemgetalstelling kunnen we dus herschrijven tot

$$\frac{n}{\ln n} = k + O\left(\frac{k}{\ln k}\right), \quad k \rightarrow \infty$$

ofwel

$$n = k \ln n (1 + O(1/\ln k)), \quad k \rightarrow \infty$$

Nu willen we nog de  $n$  uit het rechterlid elimineren.

**Het k-de priemgetal**

Toepassen van de logaritmwet geeft

$$\ln n = \ln k + \ln \ln n + O(1/\ln k), \quad k \rightarrow \infty$$

$$\begin{aligned}
 & \ln \ln n \\
 = & \{ n(\ln n)^2 \ll n^2 \} \\
 & O\left(\ln \ln \frac{n^2}{(\ln n)^2}\right) \\
 = & \{ n/\ln n \ll k \} \\
 & O(\ln \ln(k^2)) \\
 = & \{ \ln(k^2) = 2 \ln k \} \\
 & O(\ln \ln k)
 \end{aligned}$$

Invullen in de formule bovenaan geeft

$$\ln n = \ln k + O(\ln \ln k), \quad k \rightarrow \infty$$

en nogmaals invullen

$$\ln n = \ln k + \ln(\ln k + O(\ln \ln k)) + O(1/\ln k), \quad k \rightarrow \infty$$

### Het $k$ -de priemgetal

Hierin is

$$\begin{aligned}
 & \ln(\ln k + O(\ln \ln k)) \\
 = & \{ \text{rekenen} \} \\
 & \ln(\ln k + \ln(1 + O(\ln \ln k/\ln k))) \\
 = & \{ \text{logaritmwet} \} \\
 & \ln(\ln k + O(\ln \ln k/\ln k)) \\
 = & \{ \text{rekenen} \} \\
 & \ln \ln k + \ln(1 + O(\ln \ln k/(\ln k)^2)) \\
 = & \{ \text{logaritmwet} \} \\
 & \ln \ln k + O(\ln \ln k/(\ln k)^2)
 \end{aligned}$$

Substitutie in

$$\ln n = \ln k + \ln(\ln k + O(\ln \ln k)) + O(1/\ln k), \quad k \rightarrow \infty$$

geeft

$$\ln n = \ln k + \ln \ln k + O(1), \quad k \rightarrow \infty$$

### Het $k$ -de priemgetal

We hadden gevonden

$$n = k \ln n (1 + O(1/\ln k)), \quad k \rightarrow \infty$$

en wilden de  $\ln n$  uit het rechterlid verwijderen. Dat kan via

$$\ln n = \ln k + \ln \ln k + O(1), \quad k \rightarrow \infty$$

hetgeen geeft

$$n = k \ln k + k \ln \ln k + O(k), \quad k \rightarrow \infty$$

Dit is de gewenste schatting voor het  $k$ -de priemgetal.

### Bootstrapping

Terugkijkend op het voorgaande: we hadden een asymptotische recurrente betrekking voor het  $k$ -de priemgetal  $p_k$  van de vorm

$$p_k = k \ln p_k (1 + O(1/\ln k)), \quad k \rightarrow \infty$$

We hebben de  $p_k$  uit het rechterlid verwijderd en afgeleid

$$p_k = k \ln k + k \ln \ln k + O(k), \quad k \rightarrow \infty$$

door eerst uit de gegeven betrekking het zwakkere  $p_k = O(k^2)$ ,  $k \rightarrow \infty$  af te leiden en vervolgens herhaaldelijk te substitueren in het rechterlid. Deze aanpak staat bekend als 'bootstrapping'.

Nog een voorbeeld: gevraagd de coëfficiënt van  $z^n$  in de machtreeks voor

$$G(z) = \exp \sum_{k=1}^{\infty} \frac{z^k}{k^2}$$

### Recurrente betrekking

Schrijf

$$G(z) = \sum_{n=0}^{\infty} g_n z^n$$

Gevraagd wordt  $g_n$ . Differentiëren van de machtreeks geeft

$$DG(z) = \sum_{n=1}^{\infty} n g_n z^{n-1}$$

Anderzijds: differentiëren van de definitie van  $G$  geeft

$$\begin{aligned} & DG(z) \\ = & \left\{ G(z) = \exp \sum_{k=1}^{\infty} \frac{z^k}{k^2} \right\} \\ & G(z) \sum_{k=1}^{\infty} \frac{z^{k-1}}{k} \\ = & \left\{ G(z) = \sum_{l=0}^{\infty} g_l z^l \right\} \\ & \sum_{l=0}^{\infty} g_l z^l \sum_{k=1}^{\infty} \frac{z^{k-1}}{k} \\ = & \left\{ \text{convolutie} \right\} \\ & \sum_{n=1}^{\infty} \sum_{l=0}^{n-1} \frac{g_l}{n-l} z^{n-1} \end{aligned}$$

### Eerste substitutie

We hebben dus

$$\sum_{n=1}^{\infty} n g_n z^{n-1} = \sum_{n=1}^{\infty} \sum_{l=0}^{n-1} \frac{g_l}{n-l} z^{n-1}$$

Vergelijken van de coëfficiënten geeft

$$n g_n = \sum_{l=0}^{n-1} \frac{g_l}{n-l} \quad \text{voor } n \geq 1$$

Initiële zwakke benadering:  $g_n = O(1)$ ,  $n \rightarrow \infty$  (volgt met inductie uit recurrente betrekking). Substitueer dit in het rechterlid; dat geeft

$$ng_n = \sum_{l=0}^{n-1} \frac{O(1)}{n-l} = H_n O(1) = O(\ln n), \quad n \rightarrow \infty$$

dus  $g_n = O\left(\frac{\ln n}{n}\right)$ ,  $n \rightarrow \infty$ , waaruit volgt dat

$$\exists C \bullet \forall n \bullet |g_n| \leq C \frac{\ln(n+1)}{n}$$

Deze schatting kunnen we *opnieuw* in het rechterlid substitueren.

### Tweede substitutie

Voor  $n \rightarrow \infty$  is

$$\begin{aligned} & ng_n \\ = & \quad \{ \text{recurrente betrekking} \} \\ & \sum_{l=0}^{n-1} \frac{g_l}{n-l} \\ = & \quad \{ \text{splits af } l=0; \text{ gebruik verbeterde schatting voor } g_l \} \\ & \frac{g_0}{n} + \sum_{l=1}^{n-1} \frac{O(\ln(l+1))/l}{n-l} \\ = & \quad \{ g_0 = 1; \text{ monotonie van } \ln \} \\ & \frac{1}{n} + \sum_{l=1}^{n-1} \frac{O(\ln n)}{l(n-l)} \\ = & \quad \{ \text{rekenen} \} \\ & \frac{1}{n} + \sum_{l=1}^{n-1} \left( \frac{1}{l} + \frac{1}{n-l} \right) \frac{O(\ln n)}{n} \\ = & \quad \{ \text{definitie } H_n \} \\ & \frac{1}{n} + \frac{2}{n} H_{n-1} O(\ln n) \\ = & \quad \{ H_n = O(\ln n), n \rightarrow \infty \} \\ & \frac{1}{n} O((\ln n)^2) \end{aligned}$$

dus

$$g_n = O\left(\frac{(\ln n)^2}{n^2}\right), \quad n \rightarrow \infty$$

## 14 Grafen

### 14.1 Grafen

#### Gerichte grafen

Voor een verzameling  $V$  is een *binaire relatie* op  $V$  een verzameling geordende paren van elementen van  $V$ .

Voorbeeld: een binaire relatie op  $\mathbb{N}$  is de relatie *KleinerDan*, gedefinieerd door

$$(x, y) \in \text{KleinerDan} \iff x < y$$

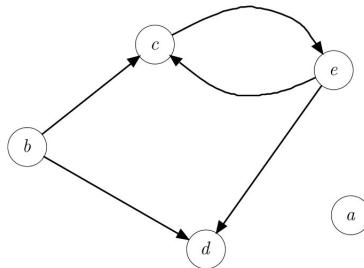
Deze relatie bevat bijvoorbeeld de paren  $(1, 2)$  en  $(3, 1000)$ , maar niet  $(2, 1)$  en niet  $(3, 3)$ .

### Gerichte graaf

Een gerichte graaf is een paar  $(V, E)$  waar  $V$  een eindige niet-lege verzameling is en  $E$  een binaire relatie op  $V$ . De elementen van  $V$  noemen we *knopen* en de elementen van  $E$  noemen we *kanten*.

### Gerichte grafen

Gerichte grafen worden gewoonlijk weergegeven door een diagram waarin de knopen door cirkeltjes en de kanten door pijlen worden aangegeven.



De hier afgebeelde graaf heeft als knopen

$$V = \{a, b, c, d, e\}$$

en als kanten

$$E = \{(b, c), (b, d), (c, e), (e, c), (e, d)\}$$

### Toepassingen in de informatica

- Computernetwerken: de knopen zijn machines in het netwerk, de kanten zijn communicatiekanalen.
- Datastructuren: de knopen zijn records, de kanten zijn pointers.
- Objectgeoriënteerd ontwerp: de knopen zijn klassen, de kanten zijn overervingsrelaties.
- Toestandsdiagrammen: de knopen zijn toestanden, de kanten zijn toestandsovergangen.
- Dataflow-diagrammen: de knopen zijn processen, de kanten zijn gegevensstromen.

### Matrixvoorstelling

Gerichte grafen kunnen ook worden gerepresenteerd door een matrix. Nummer de knopen opeenvolgend, dus neem aan dat  $V = \{1, 2, \dots, n\}$ . Dan wordt de graaf voorgesteld door de matrix

$$[[ (i, j) \in E ]]_{i,j=1}^{n,n}$$

Voorbeeld: de graaf met kanten

$$\{(2, 3), (2, 4), (3, 5), (5, 3), (5, 4)\}$$

wordt voorgesteld door de matrix

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

### Warshall's algoritme

Laat een graaf zijn voorgesteld door een boolean array  $c$  met  $c[i, j] = ((i, j) \in E)$ . Algoritme van Warshall verandert de waarde van  $c$  zodanig dat na afloop  $c[i, j]$  aangeeft of  $j$  vanuit  $i$  bereikbaar is. De Java-code is

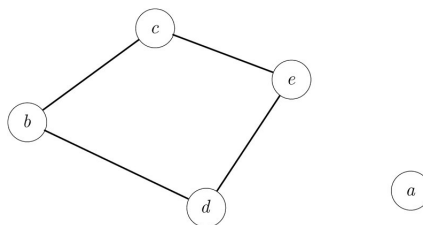
```
for (k=0; k<n; k++)
for (i=0; i<n; i++)
for (j=0; j<n; j++)
  c[i, j] = c[i, j] || c[i, k] && c[k, j];
```

Dit werkt omdat na elke slag van de iteratie over  $k$  de waarde van  $c[i, j]$  aangeeft of  $j$  vanuit  $i$  bereikbaar is via punten met nummer kleiner dan  $k$ .

### Ongerichte grafen

De kantenrelatie  $E$  heet *symmetrisch* als  $E$  voor elke  $(x, y)$  ook het omgekeerde paar  $(y, x)$  bevat. Een gerichte graaf met een symmetrische kantenrelatie correspondeert eenduidig met een *ongerichte* graaf: een ongerichte graaf  $(V, E)$  bestaat uit een niet-lege eindige verzameling  $V$  en een verzameling *ongeordende* paren  $\{x, y\}$  van elementen uit  $V$ .

Ongerichte grafen worden gewoonlijk weergegeven door een diagram waarin elk ongeordend paar  $\{x, y\}$  door een verbindingslijn zonder pijlpunt wordt aangegeven.



**De graad van een knoop**

De *in-graad* van een knoop is het aantal kanten dat in die knoop eindigt, dus

$$\text{indeg}(y) = \sum_{x \in V} [(x, y) \in E]$$

Er geldt

$$\begin{aligned} & \sum_{y \in V} \text{indeg}(y) \\ = & \quad \{\text{definitie van } \text{indeg}\} \\ & \sum_{y \in V} \sum_{x \in V} [(x, y) \in E] \\ = & \quad \{\text{eenpuntsdomein}\} \\ & \sum_{y \in V} \sum_{x \in V} \sum_{e \in E} [(x, y) = e] \\ = & \quad \{\text{dubbelsom}\} \\ & \sum_{e \in E} \sum_{y \in V} \sum_{x \in V} [(x, y) = e] \\ = & \quad \{\text{eenpuntsdomein}\} \\ & \sum_{e \in E} 1 \\ = & \quad \{\text{constante term}\} \\ & \#E \end{aligned}$$

**De graad van een knoop**

De *uit-graad* van een knoop is het aantal kanten dat in die knoop begint, dus

$$\text{outdeg}(x) = \sum_{y \in V} [(x, y) \in E]$$

Analoog aan de in-graad geldt

$$\sum_{x \in V} \text{outdeg}(x) = \#E$$

Een gevolg van deze formules is: het aantal knopen met oneven som van in- en uit-graad is even.

Bij een ongerichte graaf zijn in-graad en uit-graad aan elkaar gelijk, en spreken we kortweg over de *graad* van een knoop.

**14.2 Paden****Paden**

Voor knopen  $x$  en  $y$  is een *wandeling* van  $x$  naar  $y$  een rij knopen  $\langle x_i \rangle_{i=0}^n$  met

- $x_0 = x$
- $x_n = y$
- $\forall i \mid 0 \leq i < n \bullet (x_i, x_{i+1}) \in E$

We zeggen dat de wandeling de knopen  $x_i$  en de takken  $(x_i, x_{i+1})$  aandoet. De *lengte* van de wandeling is  $n$ , het aantal takken dat de wandeling aandoet.

Een wandeling  $\langle x_i \rangle_{i=0}^n$  heet een *pad* als alle kanten  $(x_i, x_{i+1})$  een verschillend beginpunt  $x_i$  hebben. Als er een wandeling van  $x$  naar  $y$  is, is er ook een pad: als  $0 \leq p < q < n$  met  $x_p = x_q$ , kan het deel  $\langle x_i \rangle_{i=p}^{q-1}$  uit de wandeling worden weggelaten. Een kortste wandeling van  $x$  naar  $y$  is dus noodzakelijk een pad.

**Afstand**

Knoop  $y$  is vanuit knoop  $x$  *bereikbaar* als er een pad van  $x$  naar  $y$  bestaat.

Als  $y$  vanuit  $x$  bereikbaar is, is de *afstand* van  $x$  naar  $y$  de lengte van een kortste pad van  $x$  naar  $y$ .

Een graaf heet *samenhangend* als elke knoop vanuit elke andere knoop bereikbaar is.

Een *cykel* is een pad  $\langle x_i \rangle_{i=0}^n$  met  $x_n = x_0$ . Een graaf heet *acyclisch* als de graaf geen cyclen bevat.

**Algoritme van Dijkstra**

Bepaalt de afstand van knoop  $x$  naar knoop  $y$  in een samenhangende gerichte graaf.

1. Kleur alle knopen wit
2. Label alle punten met  $\infty$ , maar  $x$  met 0
3. Zolang  $y$  nog wit is:
  - (a) Kies een wit punt  $w$  met minimaal label, zeg  $l$
  - (b) Kleur  $w$  zwart
  - (c) Vervang voor alle  $z$  met  $(w, z) \in E$  het label door  $l + 1$  als dat lager is

Dit werkt omdat voor alle zwarte punten het label de afstand vanaf  $x$  voorstelt. Gaat ook goed als kanten een gewicht hebben. Vergelijk routeplanner in IMP.

De buitenste herhalingsopdracht wordt ten hoogste  $\#V$  maal uitgevoerd. Bij een efficiënte implementatie is de totale rekestijd  $O((\#E + \#V) \ln \#V)$ . Zie voor volledige behandeling de cursus Algoritmiek.

Animatie: <http://www.cs.uu.nl/docs/vakken/wis/wis1403.gif> (bron: Combinatorica).

**Hamiltoncykels**

Een *Hamiltoncykel* is een cykel die elke knoop van de graaf precies éénmaal bevat.

Er is geen eenvoudig criterium om te bepalen of een graaf een Hamiltoncykel heeft; er is geen efficiënt algoritme om een Hamiltoncykel te vinden. Het vinden van een Hamiltoncykel met minimaal gewicht staat bekend als het *Traveling Salesman Problem*. De best bekende algoritmen hebben complexiteit  $\Omega(e^n)$ , en zijn dus niet bruikbaar behalve voor heel kleine  $n$ .

**14.3 Bomen****Bomen**

Een *boom* is een samenhangende acyclische ongerichte graaf.

Toepassingen in de informatica:

- Compilers: weergave van de structuur van een expressie
- Bestandssystemen: structuur van directories en bestanden

- Toepassingsprogramma's: structuur van documenten, e-mail folders enz.
- Beslissingsondersteuning: structuur van keuzeprocessen

### Stelling

Voor een boom  $(V, E)$  geldt  $\#E = \#V - 1$ .

### Bomen

Bewijs van de stelling: inductie naar  $\#E$ . Basis: als  $\#E = 0$ , zijn er geen kanten. Omdat de boom samenhangend is, kan er dan slechts 1 knoop zijn. (In de definitie van graaf staat dat er ook *ten minste* 1 knoop is.)

Stap: zij  $\#E = n > 0$  en stel dat de uitspraak waar is voor alle bomen met  $n - 1$  kanten. Omdat de boom geen cykels bevat, moet er een knoop van graad 1 zijn. Als we deze knoop en de unieke kant die daar begint verwijderen, ontstaat een boom met  $n - 1$  kanten en  $\#V - 1$  knopen. Uit de inductiehypothese volgt dan dat  $n - 1 = \#V - 2$ .  $\square$

### Algoritme van Prim

Gegeven is een samenhangende ongerichte graaf met gewichten toegekend aan de kanten. Algoritme van Prim construeert een boom die alle knopen bevat en minimaal gewicht heeft.

1. Kleur alle knopen en kanten wit
2. Kleur een willekeurig punt zwart
3. Zolang er nog witte knopen zijn:
  - (a) Zij  $e$  een kant van minimaal gewicht die een zwart punt met een wit punt verbindt
  - (b) Kleur  $e$  en zijn witte eindknoop zwart

Aan het eind vormen de zwarte knopen en kanten de gevraagde boom. Dit werkt omdat het zwarte gedeelte steeds een boom is die tot een minimale opspannende boom kan worden uitgebreid.

De complexiteit is, net als Dijkstra's algoritme,  $O((\#E + \#V) \ln \#V)$  (zie cursus Algoritmiek).

Animatie: <http://www.cs.uu.nl/docs/vakken/wis/Prim>

## 14.4 Planariteit

### Stelling van Euler

Een *planaire* graaf is een ongerichte graaf die op een plat vlak getekend kan worden.

### Stelling van Euler

Zij  $(V, E)$  een samenhangende planaire graaf waarvan de kanten het platte vlak in  $f$  gebieden verdelen. Dan geldt

$$\#V - \#E + f = 2$$

Bewijs: inductie naar  $\#E - \#V$ . Omdat de graaf samenhangend is, geldt  $\#E - \#V \geq -1$ .

Basis:  $\#E - \#V = -1$ . Dan bevat de graaf geen cyclen en dus is  $f = 1$ .

### Stelling van Euler

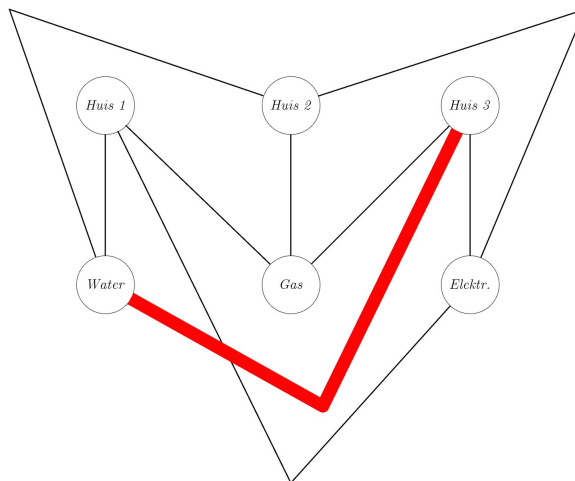
Stap: Zij  $\#E - \#V = n > -1$ . Dan is de graaf geen boom en bevat dus een cykel. Verwijder een kant uit deze cykel: dat geeft een nieuwe samenhangende planaire graaf  $(V, E')$  met  $\#E' = \#E - 1$  waarvan de kanten het platte vlak in  $f - 1$  gebieden verdelen. Dan

$$\begin{aligned} & \#V - \#E + f \\ = & \quad \{ \text{rekenen} \} \\ & \#V - \#E' + f - 1 \\ = & \quad \{ \text{inductiehypothese} \} \\ & 2 \end{aligned}$$

□

### Stelling van Euler

Drie huizen moeten elk worden verbonden met water, gas en elektriciteit. Is het mogelijk dit zo te doen dat de leidingen elkaar niet kruisen?



### Stelling van Euler

Het aantal knopen is  $\#V = 6$ , het aantal kanten is  $\#E = 9$  (drie huizen die elk met drie nutsbedrijven moeten worden verbonden). Als de resulterende graaf planair zou zijn, zou deze volgens de stelling van Euler het vlak verdelen in  $2 - 6 + 9 = 5$  gebieden.

De 9 kanten liggen elk op de rand van 2 gebieden, dus de 5 gebieden kunnen niet elk door minstens 4 kanten worden begrensd (omdat  $5 \cdot 4 > 2 \cdot 9$ ). Er is dus een gebied dat

door 3 kanten wordt begrensd, maar dat betekent dat twee huizen of twee nutsbedrijven rechtstreeks verbonden zijn.

### **Stelling van Euler**

Het gegeven dat een graaf planair is, impliceert geenzins dat de layout ook uniek is. Eenzelfde graaf kan verschillende planaire layouts hebben, maar uit de stelling van Euler volgt dat de verschillende tekeningen van een graaf een ding gemeen hebben: evenveel vlakken! Immers,  $\#V$  en  $\#E$  liggen vast.

Een algoritme om in lineaire tijd de planariteit van een graaf te testen is in 1971 gevonden door Robert Tarjan en John E. Hopcroft. In 1986 ontvingen zij hiervoor de Turing Award.