



met de computer bewijzen correct bewijzen

Freek Wiedijk

Raboud Universiteit Nijmegen

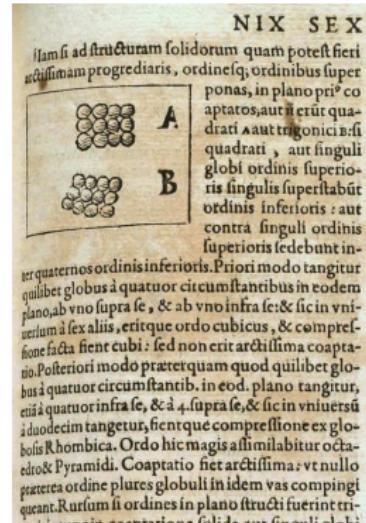
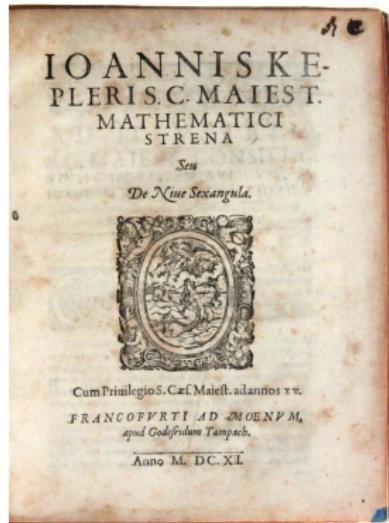
Vakantiecursus Wiskunde

Eindhoven, 26 augustus 2017  
Amsterdam, 2 september 2017

# het vermoeden van Kepler

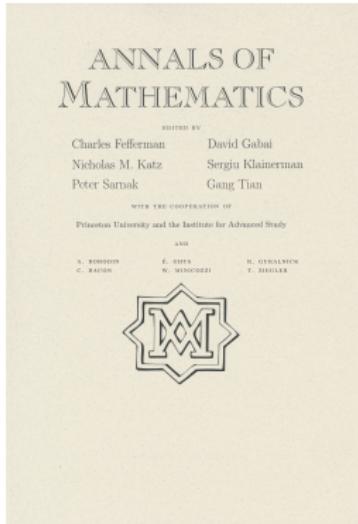
## Johannes Kepler en de zeshoekige sneeuwvlok

*Strena Seu De Nive Sexangula*, 1611



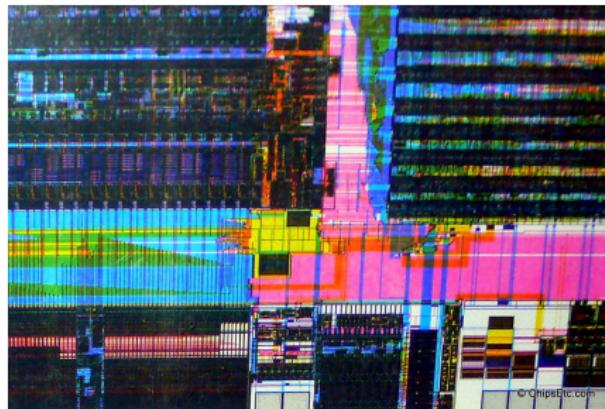
# Tom Hales en het Flyspeck-project

---



# John Harrison, Intel en HOL Light

---



## efficiënt bollen stapelen

verschillende dichtste stapelingen

---

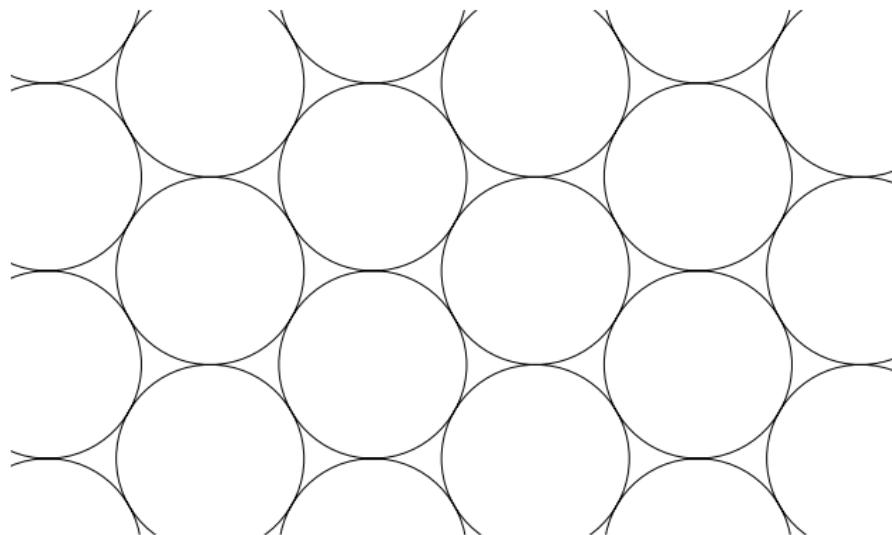
$$\frac{\pi}{\sqrt{18}} = 74,0480\dots\%$$

FCC = face-centered cubic = kubisch vlakgecentreerd

HCP = hexagonal close-packed = hexagonale dichtst

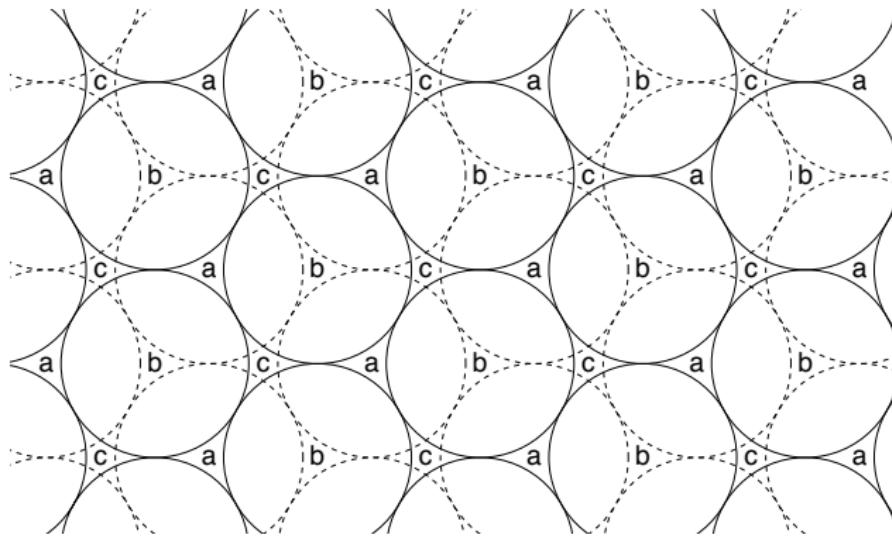
## hexagonale lagen

---



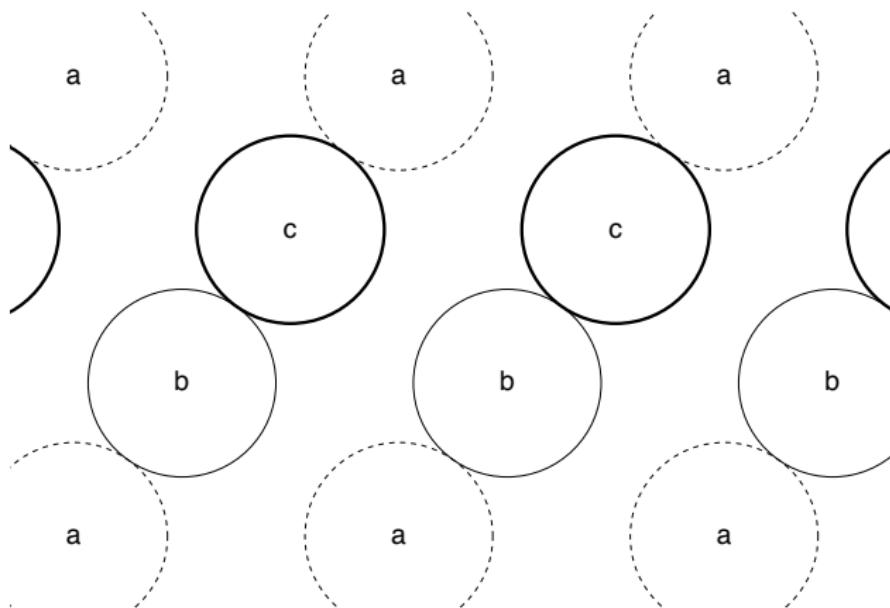
## hexagonale lagen

---



## hexagonale lagen

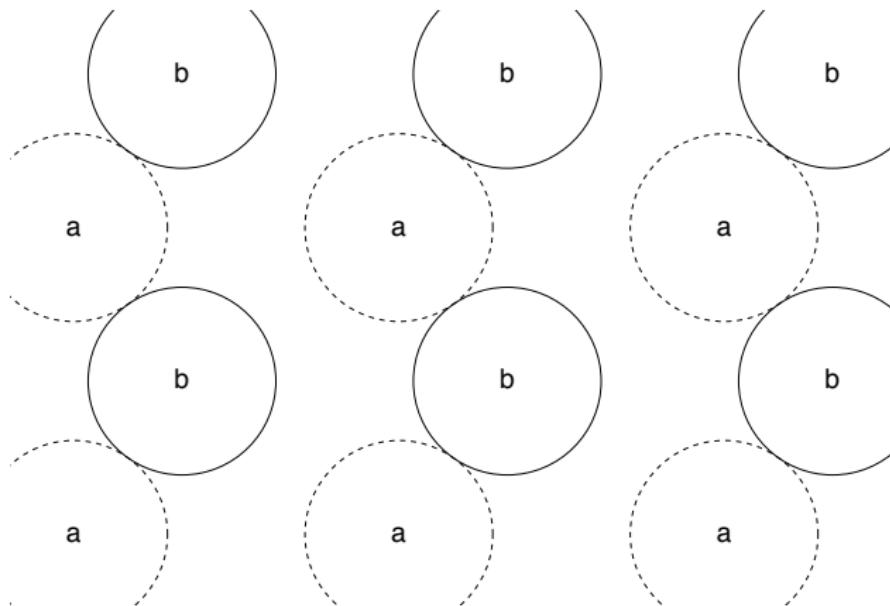
---



FCC

## hexagonale lagen

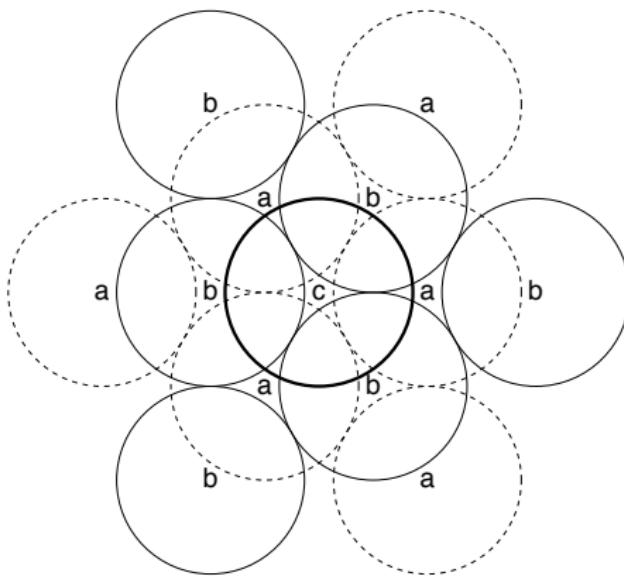
---



HCP

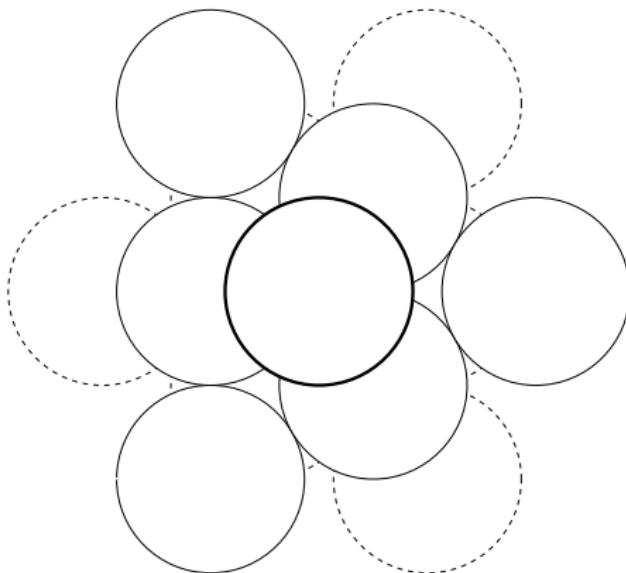
## kubisch vlakgecentreerd

---



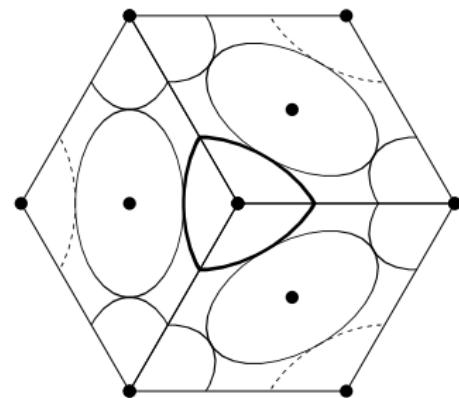
## kubisch vlakgecentreerd

---



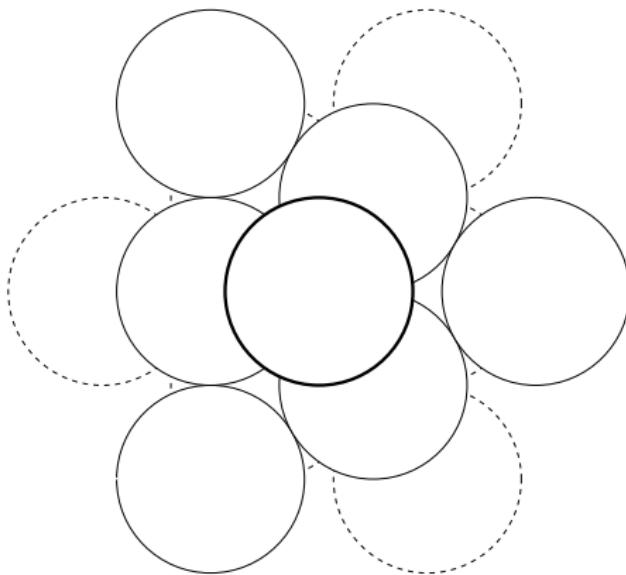
## kubisch vlakgecentreerd

---



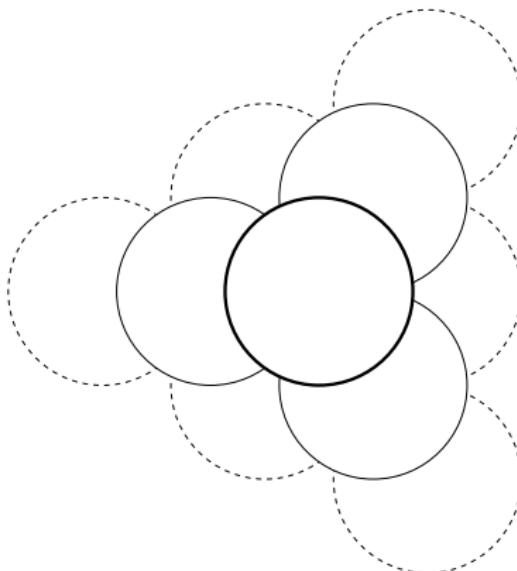
## kubisch vlakgecentreerd

---



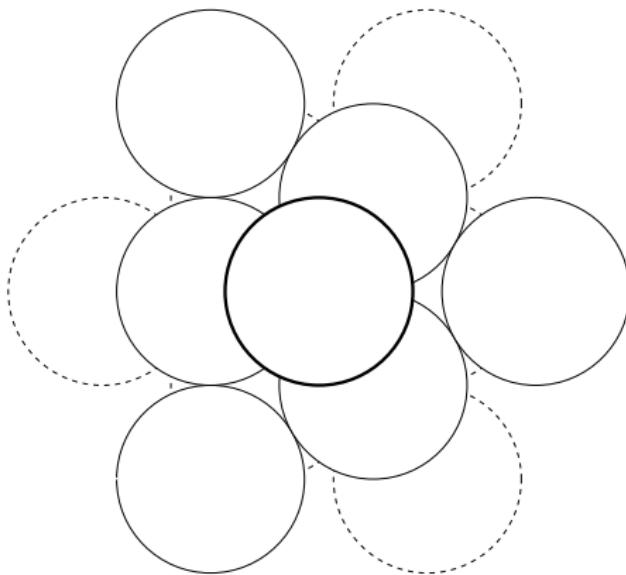
## kubisch vlakgecentreerd

---



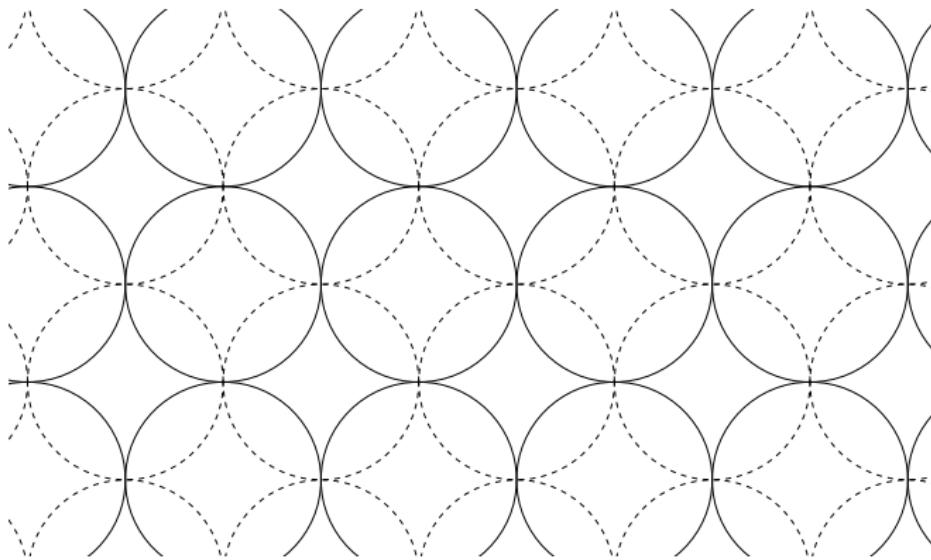
## vierkante lagen

---



## vierkante lagen

---



## het Flyspeck-bewijs

### de precieze formulering

---

voor iedere stapeling van bollen met straal één bestaat er een reëel getal  $c$  zodat voor het aantal middelpunten  $N$  van de gestapelde bollen binnen een groeiende grote bol met straal  $R$  geldt dat

$$N \leq \frac{\pi}{\sqrt{18}} R^3 + cR^2$$

## het Flyspeck-bewijs

### de precieze formulering

---

voor iedere stapeling van bollen met straal één bestaat er een reëel getal  $c$  zodat voor het aantal middelpunten  $N$  van de gestapelde bollen binnen een groeiende grote bol met straal  $R$  geldt dat

$$N \leq \frac{\pi}{\sqrt{18}} R^3 + cR^2$$

volume gestapelde bollen:  $N \cdot \frac{4}{3}\pi$

volume groeiende grote bol:  $\frac{4}{3}\pi R^3$

---

verhouding volumes:  $\frac{N \cdot \frac{4}{3}\pi}{\frac{4}{3}\pi R^3} = \frac{N}{R^3}$

## het Flyspeck-bewijs

### de precieze formulering

---

voor iedere stapeling van bollen met straal één bestaat er een reëel getal  $c$  zodat voor het aantal middelpunten  $N$  van de gestapelde bollen binnen een groeiende grote bol met straal  $R$  geldt dat

$$N \leq \frac{\pi}{\sqrt{18}} R^3 + cR^2$$

volume gestapelde bollen:  $N \cdot \frac{4}{3}\pi$

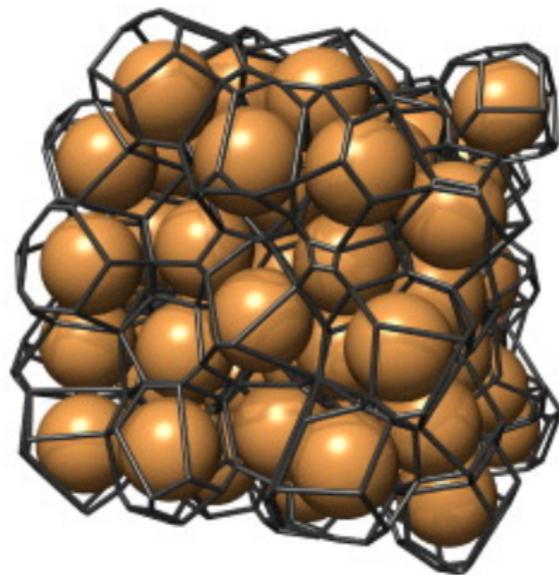
volume groeiende grote bol:  $\frac{4}{3}\pi R^3$

---

verhouding volumes:  $\frac{N \cdot \frac{4}{3}\pi}{\frac{4}{3}\pi R^3} = \frac{N}{R^3} \leq \frac{\pi}{\sqrt{18}} + \frac{c}{R}$

## Voronoi-cellen

---



## verwaarloosbare FCC-compatible functies

---

$$4\sqrt{2} = 5,55685\dots$$

volume Voronoi-cel van de FCC-stapeling

voor iedere stapeling  $V_S$  bestaat er een functie  $G(v)$  met

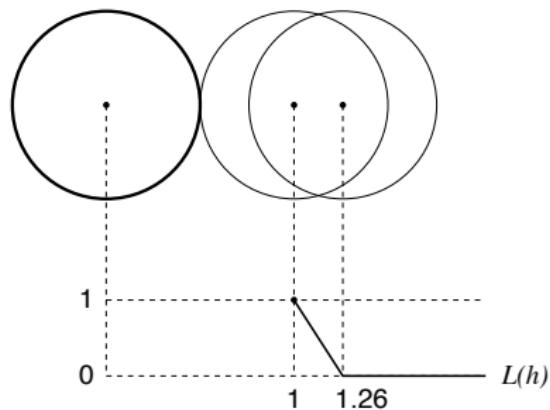
$$\sum_{v \in V_S(0,R)} G(v) \leq c_1 R^2$$

$$\text{vol}(\Omega(V_S, v)) \geq 4\sqrt{2} - G(v)$$

## de lokale annulus-ongelijkheid

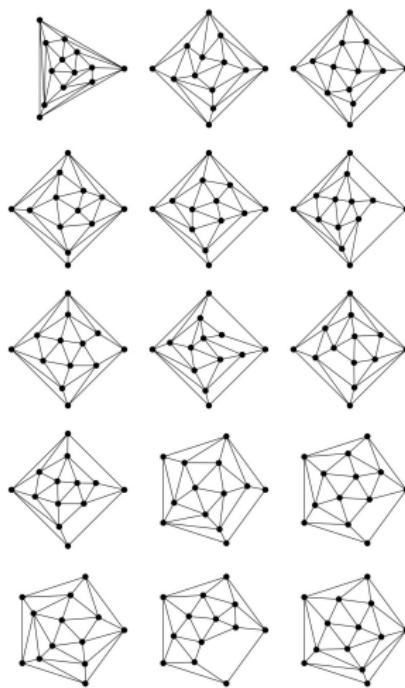
---

$$\sum_{v \in V_S} L(h(v)) \leq 12$$



## 19.715 tamme grafen

---



## 23.242 niet-lineaire ongelijkheden

---

$$\tan\left(\frac{\pi}{2} - 0.74\right) > \frac{-x_1x_3 - x_2x_4 + x_1x_5 + x_3x_6 - x_5x_6 + x_2(-x_2 + x_1 + x_3 - x_4 + x_5 + x_6)}{\sqrt{4x_2 \left( x_2x_4(-x_2 + x_1 + x_3 - x_4 + x_5 + x_6) + x_1x_5(x_2 - x_1 + x_3 + x_4 - x_5 + x_6) + x_3x_6(x_2 + x_1 - x_3 + x_4 + x_5 - x_6) - x_1x_3x_4 - x_2x_3x_5 - x_2x_1x_6 - x_4x_5x_6 \right)}}$$

## HOL Light

een lemma uit het boek van Hales

---

*Dense Sphere Packings: a Blueprint for Formal Proofs*

**Lemma 2.32** (Cauchy–Schwarz inequality) [JJJKJALK]

$$|\mathbf{u} \cdot \mathbf{v}| \leq \|\mathbf{u}\| \|\mathbf{v}\|.$$

Furthermore, the case  $\pm\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \|\mathbf{v}\|$  of equality holds exactly when  $\|\mathbf{v}\|\mathbf{u} = \pm\|\mathbf{u}\|\mathbf{v}$  (with matching signs).

*Proof* This is an exercise in real arithmetic. Let  $\mathbf{w} = \|\mathbf{v}\|\mathbf{u} \pm \|\mathbf{u}\|\mathbf{v}$ . The expansion of  $\mathbf{w} \cdot \mathbf{w}$  gives

$$0 \leq \mathbf{w} \cdot \mathbf{w} = 2\|\mathbf{u}\|^2\|\mathbf{v}\|^2 \pm 2\|\mathbf{u}\| \|\mathbf{v}\|(\mathbf{u} \cdot \mathbf{v}) = 2\|\mathbf{u}\| \|\mathbf{v}\|(\|\mathbf{u}\| \|\mathbf{v}\| \pm (\mathbf{u} \cdot \mathbf{v})).$$

If  $2\|\mathbf{u}\| \|\mathbf{v}\| = 0$ , then  $\mathbf{u}$  or  $\mathbf{v}$  is zero, and the result easily ensues. Otherwise divide both sides of the inequality by the positive number  $2\|\mathbf{u}\| \|\mathbf{v}\|$  to get the result.  $\square$

## hetzelfde lemma in HOL Light

---

```
let NORM_CAUCHY_SCHWARZ = prove
  ('!(x:real^N) y. x dot y <= norm(x) * norm(y)',,
  REPEAT STRIP_TAC THEN MAP_EVERY ASM_CASES_TAC
    ['norm(x:real^N) = &0'; 'norm(y:real^N) = &0'] THEN
  ASM_SIMP_TAC[NORM_EQ_0_IMP; DOT_LZERO; DOT_RZERO;
    REAL_MUL_LZERO; REAL_MUL_RZERO] THEN
  MP_TAC(ISPEC 'norm(y:real^N) % x - norm(x:real^N) % y' DOT_POS_LE) THEN
  REWRITE_TAC[DOT_RSUB; DOT_LSUB; DOT_LMUL; DOT_RMUL; GSYM NORM_POW_2;
    REAL_POW_2; REAL_LE_refl] THEN
  REWRITE_TAC[DOT_SYM; REAL_ARITH
    '&0 <= y * (y * x * x - x * d) - x * (y * d - x * y * y) <=>
    x * y * d <= x * y * x * y'] THEN
  ASM_SIMP_TAC[REAL_LE_LMUL_EQ; REAL_LT_LE; NORM_POS_LE]);;
```

## hetzelfde lemma in HOL Light

---

```
let NORM_CAUCHY_SCHWARZ = prove
  ('!(x:real^N) y. x dot y <= norm(x) * norm(y)',,
  REPEAT STRIP_TAC THEN MAP_EVERY ASM_CASES_TAC
    ['norm(x:real^N) = &0'; 'norm(y:real^N) = &0'] THEN
  ASM_SIMP_TAC[NORM_EQ_0_IMP; DOT_LZERO; DOT_RZERO;
    REAL_MUL_LZERO; REAL_MUL_RZERO] THEN
  MP_TAC(ISPEC 'norm(y:real^N) % x - norm(x:real^N) % y' DOT_POS_LE) THEN
  REWRITE_TAC[DOT_RSUB; DOT_LSUB; DOT_LMUL; DOT_RMUL; GSYM NORM_POW_2;
    REAL_POW_2; REAL_LE_refl] THEN
  REWRITE_TAC[DOT_SYM; REAL_ARITH
    '&0 <= y * (y * x * x - x * d) - x * (y * d - x * y * y) <=>
    x * y * d <= x * y * x * y'] THEN
  ASM_SIMP_TAC[REAL_LE_LMUL_EQ; REAL_LT_LE; NORM_POS_LE]);;
```

## een klein voorbeeld: bewijs met inductie

---

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

## een klein voorbeeld: bewijs met inductie

---

$$\sum_{i=1}^0 i = \frac{0(0+1)}{2}$$

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

$$\Downarrow$$
$$\sum_{i=1}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}$$

## een klein voorbeeld: bewijs met inductie

---

$$\sum_{i=1}^0 i = \frac{0(0+1)}{2}$$

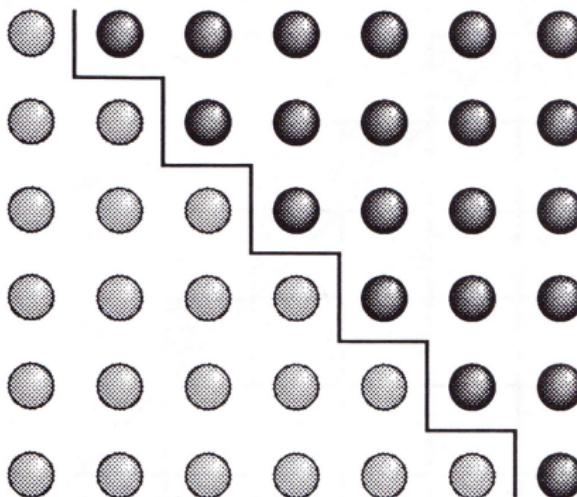
$$\sum_{i=1}^n i = \frac{n(n+1)}{2}$$

$$\Downarrow$$
$$\sum_{i=1}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}$$

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^n i + (n+1) = \left(\frac{n(n+1)}{2}\right) + (n+1) = \frac{(n+1)((n+1)+1)}{2}$$

## Proofs without Words: Exercises in Visual Thinking

---



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

## HOL Light sessie: doelen en tactieken

---

#

## HOL Light sessie: doelen en tactieken

---

```
# g `!n. nsum (1..n) (\i. i) = (n*(n + 1)) DIV 2`;;
val it : goalstack = 1 subgoal (1 total)

`!n. nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2`

#
```

## HOL Light sessie: doelen en tactieken

---

```
# g '!n. nsum (1..n) (\i. i) = (n*(n + 1)) DIV 2;;  
val it : goalstack = 1 subgoal (1 total)  
  
'!n. nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2'  
  
# e INDUCT_TAC;;  
val it : goalstack = 2 subgoals (2 total)  
  
0 ['nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2']  
  
'nsum (1..SUC n) (\i. i) = (SUC n * (SUC n + 1)) DIV 2'  
  
'nsum (1..0) (\i. i) = (0 * (0 + 1)) DIV 2'  
  
#
```

## HOL Light sessie: doelen en tactieken

---

```
# g '!n. nsum (1..n) (\i. i) = (n*(n + 1)) DIV 2;;  
val it : goalstack = 1 subgoal (1 total)  
  
'!n. nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2'  
  
# e INDUCT_TAC;;  
val it : goalstack = 2 subgoals (2 total)  
  
0 ['nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2']  
  
'nsum (1..SUC n) (\i. i) = (SUC n * (SUC n + 1)) DIV 2'  
  
'nsum (1..0) (\i. i) = (0 * (0 + 1)) DIV 2'  
  
# NSUM_CLAUSES_NUMSEG;;  
val it : thm =  
|- (!m. nsum (m..0) f = (if m = 0 then f 0 else 0)) /\  
  (!m n.  
    nsum (m..SUC n) f =  
    (if m <= SUC n then nsum (m..n) f + f (SUC n) else nsum (m..n) f))  
#
```

## HOL Light sessie: doelen en tactieken

---

```
# g '!n. nsum (1..n) (\i. i) = (n*(n + 1)) DIV 2;;  
val it : goalstack = 1 subgoal (1 total)  
  
'!n. nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2'  
  
# e INDUCT_TAC;;  
val it : goalstack = 2 subgoals (2 total)  
  
0 ['nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2']  
  
'nsum (1..SUC n) (\i. i) = (SUC n * (SUC n + 1)) DIV 2'  
  
'nsum (1..0) (\i. i) = (0 * (0 + 1)) DIV 2'  
  
# NSUM_CLAUSES_NUMSEG;;  
val it : thm =  
|- (!m. nsum (m..0) f = (if m = 0 then f 0 else 0)) /\  
  (!m n.  
    nsum (m..SUC n) f =  
    (if m <= SUC n then nsum (m..n) f + f (SUC n) else nsum (m..n) f))  
# e (REWRITE_TAC[NSUM_CLAUSES_NUMSEG]);;  
val it : goalstack = 1 subgoal (2 total)  
  
'(if 1 = 0 then 0 else 0) = (0 * (0 + 1)) DIV 2'  
  
#
```

## HOL Light sessie: doelen en tactieken

---

```
val it : goalstack = 1 subgoal (2 total)

` (if 1 = 0 then 0 else 0) = (0 * (0 + 1)) DIV 2 `

# e ARITH_TAC;;
val it : goalstack = 1 subgoal (1 total)

0 [| ` nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2 ` |]

` nsum (1..SUC n) (\i. i) = (SUC n * (SUC n + 1)) DIV 2 `

#
```

## HOL Light sessie: doelen en tactieken

---

```
val it : goalstack = 1 subgoal (2 total)

` (if 1 = 0 then 0 else 0) = (0 * (0 + 1)) DIV 2 `

# e ARITH_TAC;;
val it : goalstack = 1 subgoal (1 total)

0 [| `nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2 ` |]

`nsum (1..SUC n) (\i. i) = (SUC n * (SUC n + 1)) DIV 2 `

# e (REWRITE_TAC[NSUM_CLAUSES_NUMSEG]);;
val it : goalstack = 1 subgoal (1 total)

0 [| `nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2 ` |]

` (if 1 <= SUC n then nsum (1..n) (\i. i) + SUC n else nsum (1..n) (\i. i)) =
 (SUC n * (SUC n + 1)) DIV 2 `

#
```

## HOL Light sessie: doelen en tactieken

---

```
val it : goalstack = 1 subgoal (1 total)

0 [‘nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2’]

‘(if 1 <= SUC n then nsum (1..n) (\i. i) + SUC n else nsum (1..n) (\i. i)) =
(SUC n * (SUC n + 1)) DIV 2’

# e (ASM_REWRITE_TAC []);;
val it : goalstack = 1 subgoal (1 total)

0 [‘nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2’]

‘(if 1 <= SUC n then (n * (n + 1)) DIV 2 + SUC n else (n * (n + 1)) DIV 2) =
(SUC n * (SUC n + 1)) DIV 2’

#
```

## HOL Light sessie: doelen en tactieken

---

```
val it : goalstack = 1 subgoal (1 total)

0 [‘nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2’]

‘(if 1 <= SUC n then nsum (1..n) (\i. i) + SUC n else nsum (1..n) (\i. i)) =
(SUC n * (SUC n + 1)) DIV 2’

# e (ASM_REWRITE_TAC []);
val it : goalstack = 1 subgoal (1 total)

0 [‘nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2’]

‘(if 1 <= SUC n then (n * (n + 1)) DIV 2 + SUC n else (n * (n + 1)) DIV 2) =
(SUC n * (SUC n + 1)) DIV 2’

# e ARITH_TAC;;
val it : goalstack = No subgoals

#
```

## HOL Light sessie: doelen en tactieken

---

```
val it : goalstack = 1 subgoal (1 total)

0 [‘nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2’]

‘(if 1 <= SUC n then nsum (1..n) (\i. i) + SUC n else nsum (1..n) (\i. i)) =
(SUC n * (SUC n + 1)) DIV 2’

# e (ASM_REWRITE_TAC []);
val it : goalstack = 1 subgoal (1 total)

0 [‘nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2’]

‘(if 1 <= SUC n then (n * (n + 1)) DIV 2 + SUC n else (n * (n + 1)) DIV 2) =
(SUC n * (SUC n + 1)) DIV 2’

# e ARITH_TAC;;
val it : goalstack = No subgoals

# top_thm();;
val it : thm = |- !n. nsum (1..n) (\i. i) = (n * (n + 1)) DIV 2
#
```

## HOL Light sessie: doelen en tactieken

---

```
let TRIANGULAR_SUM = prove
  ('!n. nsum (1..n) (\i. i) = (n*(n + 1)) DIV 2',
  INDUCT_TAC THENL
  [REWRITE_TAC[NSUM_CLAUSES_NUMSEG] THEN
  ARITH_TAC;
  REWRITE_TAC[NSUM_CLAUSES_NUMSEG] THEN
  ASM_REWRITE_TAC[] THEN
  ARITH_TAC]);;
```

## HOL Light sessie: doelen en tactieken

---

```
let TRIANGULAR_SUM = prove
(`!n. nsum (1..n) (\i. i) = (n*(n + 1)) DIV 2`,
  INDUCT_TAC THEN
  ASM_REWRITE_TAC [NSUM_CLAUSES_NUMSEG] THEN
  ARITH_TAC);;
```

# formele bewijzen in de computer

Coq en Isabelle

---



## formalisaties van George Gonthier

---



iedere vlakke kaart is kleurbaar met vier kleuren

iedere eindige groep van oneven orde is oplosbaar

## het criterium van N.G. de Bruijn

---



eenvoudige checker die volledige wiskundige correctheid garandeert

## de drie revoluties in de wiskunde

---



bewijzen



rigoreus  
bewijzen



formeel  
rigoreus  
bewijzen

## table of contents

### contents

---

het vermoeden van Kepler

efficiënt bollen stapelen

het Flyspeck-bewijs

HOL Light

formele bewijzen in de computer

table of contents