Codes en Projectieve vlakken

Jozefien D'haeseleer en Robin Simoens

Unimath 2024

UNIVERSITEIT GENT

Overzicht

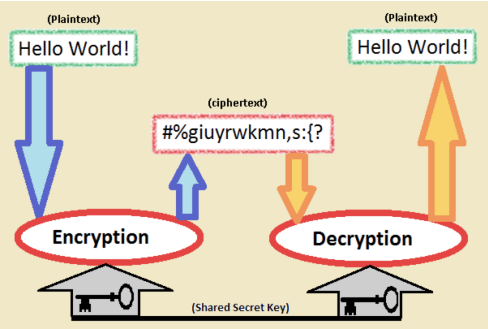
1. Codeertheorie
2. Economische Toepassingen
3. Projectieve Vlakken
4. Latijnse Vierkanten

Codeertheorie

4 Codeertheorie

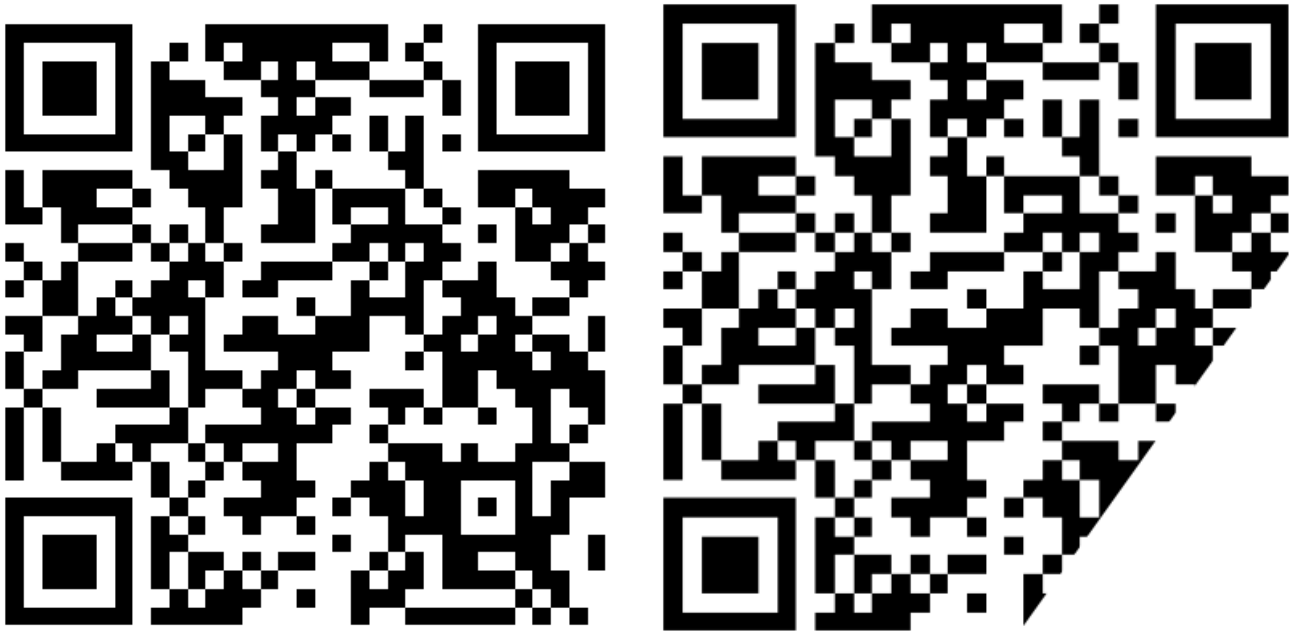
5 Codeertheorie vs Cryptografie

- Codeertheorie: boodschap duidelijk maken
- Cryptografie: boodschap verbergen (voor buitenstaanders)



Coderehtoerie, neit te vewrareren mte cyrptgorafie, is een onerddeel vna de infroamitetheorie dat zcih rciht op hte teovoeegn van gceoderede infromatie, waradoor deze bteer beshcremd is tegen moegljike fuoten dei knunen oprteden tjidens hte vezrenden ovre een onebtruowbaar kannaal.

Codeertheorie, niet te verwarren met cryptografie, is een onderdeel van de informatietheorie dat zich richt op het toevoegen van gecodeerde informatie, waardoor deze beter beschermd is tegen mogelijke fouten die kunnen optreden tijdens het verzenden over een onbetrouwbaar kanaal.



Inleidende voorbeelden

9 Code op zee

Noord:	00
Oost:	01
Zuid:	10
West:	11

10 Code op zee

Noord:	000
Oost:	011
Zuid:	101
West:	110

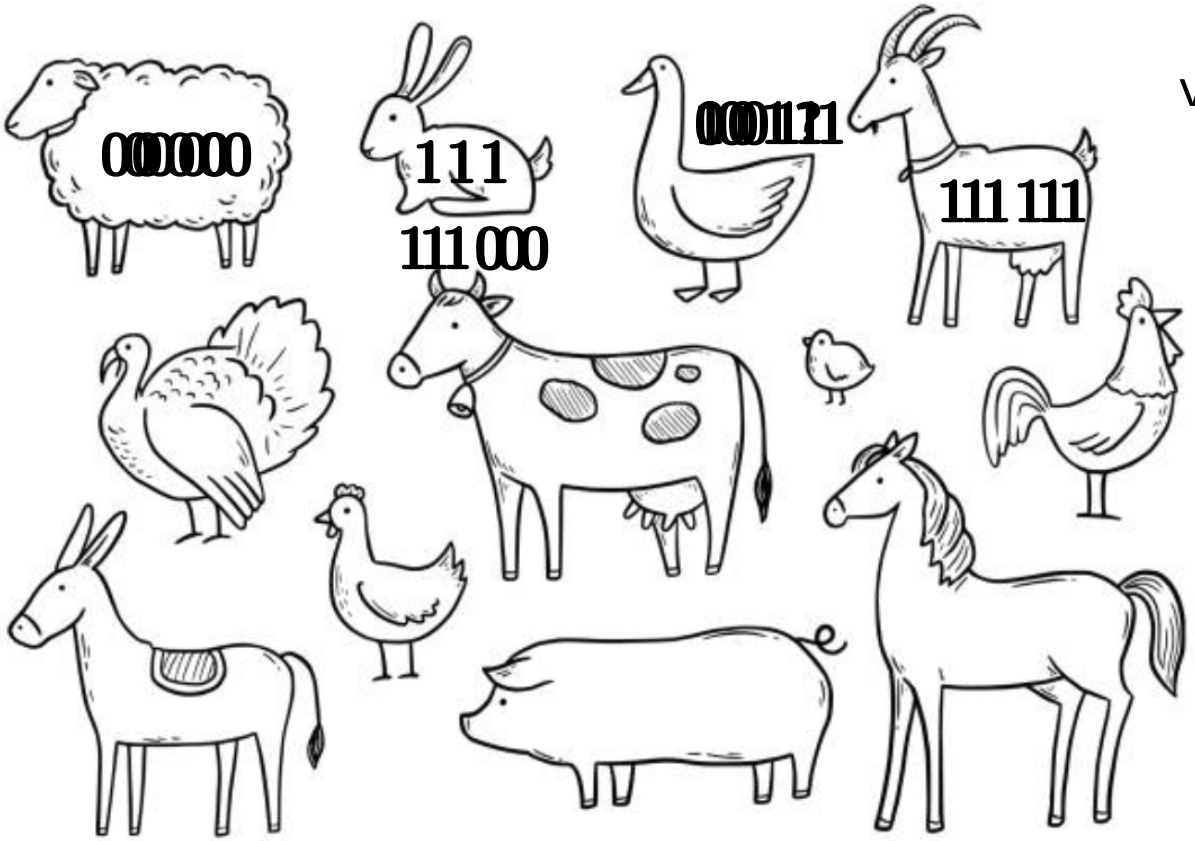
$010 \to 000, 011$ of 110?
1-fout detecterend

11 Code op zee

Noord:	000000
Oost:	011011
Zuid:	101101
West:	110110

$010000 \rightarrow 000000$
$011000 \rightarrow 000000$ of 011011?
3-fout detecterend
1-fout verbeterend!

12 Code van het dierenrijk



Elke twee codewoorden moeten verschillen in minstens 3 posities.

1100000101001110
0111010101111101
0001010110101001
0101010101010111
0100100100011100
0001111010110001
1001110010011010
0010111011110001
1101011000010100
0010001111011111
1001011010000101
0010101110101010
1111101000100001
0101010010101011
0010011010001111
0011101011010100

13 Codeertheorie

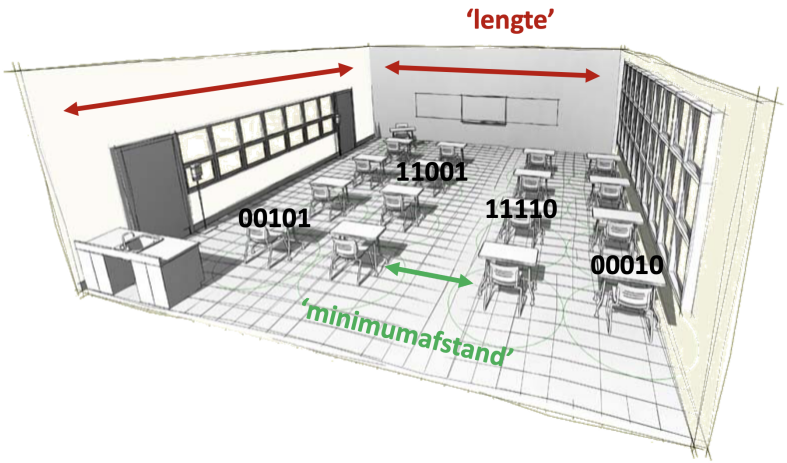
Goede code

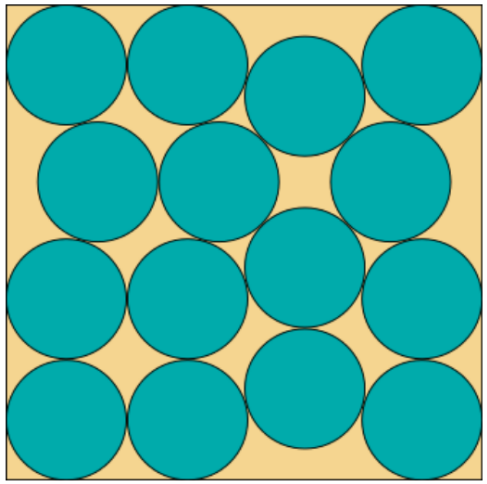
- De code bevat zo veel mogelijk codewoorden.
- De codewoorden zijn zo kort mogelijk.
- Codewoorden zijn zo 'verschillend' mogelijk.

- De afstand tussen codewoorden: aantal posities waarin deze twee verschillen.
- Afstand tussen 1101000 en 1110010?
- Minimumafstand

14 Hoofdprobleem Codeertheorie

Gegeven de lengte (vb 5) en minimumafstand (vb 3):
Hoeveel codewoorden kunnen we maximaal construeren?

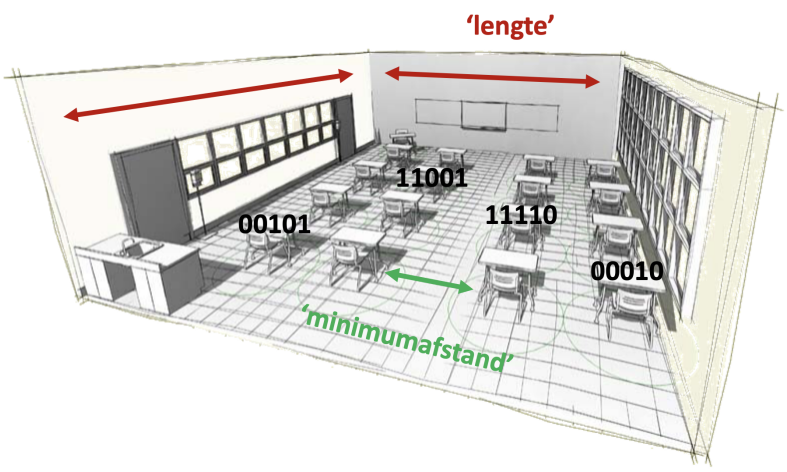


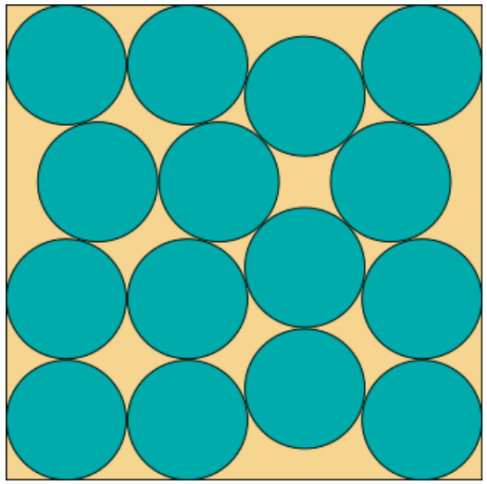


15 Codeertheorie

Verklaar de volgende uitspraken.

- Zij t de minimumafstand van de code C, dan kan C $t-1$ fouten detecteren.
- Zij $t = 2s+1$ de minimumafstand van de code C, dan kan de code s fouten verbeteren.





16 De Fanocode

- 16 codewoorden
- 1-fout verbeterend
- 7 bits.

0000000	1111111
1101000	0010111
0110100	1001011
0011010	1100101
0001101	1110010
1000110	0111001
0100011	1011100
1010001	0101110

Hoeveel codewoorden dien je te onthouden om alle 16 codewoorden van de Fanocode te kunnen bekomen?

$1011001 \rightarrow 1010001$

Economische toepassingen

18 Bankbiljetten

Serienummer: S23293098133

19 Bankbiljetten

Serienummer: S23293098133

Vervang de letter door positie in alfabet+1, en tel hierbij het getal op.
Het bekomen getal α moet deelbaar zijn door 9.

S: 19de letter; dus $\alpha = 19 + 1 + 23293098133$.
Is dit getal deelbaar door 9?

20 Deelbaarheid door 9

Wanneer is een getal deelbaar door 9?

Een getal is deelbaar door 9 als en slechts als de som van zijn cijfers deelbaar is door 9.

21 Rekeningnummers

Oude rekeningnummers

- Van de vorm $abc - defghij - kl$
- Controle: $abcdefghij - kl$ is een veelvoud van 97

Voorbeeld

- $000 - 0000012 - 12$
- $000 - 0000194 - 01$ is geen correct rekeningnummer. Stel dat er één fout gemaakt is. Hoe kan je die terugvinden?
- $000 - 0000195 - 01$ of $000 - 0000194 - 00$ zijn correcte rekeningnummers.

22 Rekeningnummers

Nieuwe rekeningnummers

- Van de vorm BExx abcd efgh ijkl
- Controlegetal xx: vervang de letters door de positie in het alfabet +9, plaats xx achteraan.
  Resulterend getal -1 is een veelvoud van 97.

Voorbeeld

BE17 0000 0000 2121

B $\rightarrow$ 2 $\rightarrow$ 11

E $\rightarrow$ 5 $\rightarrow$ 14

$2121111417 - 1 = 97 \cdot 21867128$

23 Rijksregisternummers

Een RRN bevat veel informatie. De structuur van een RRN is als volgt: de eerste 6 cijfers komen overeen met de geboortedatum, in de vorm JJMMDD, dus eerst het jaartal, dan de maand, en dan de dag. De volgende 3 cijfers zijn als volgt bepaald: voor een man is dit een oneven getal, voor een vrouw een even getal. Verder zijn deze 3 cijfers een teller voor de geboortes van die dag. De 10de vrouw die op een bepaalde dag geboren wordt, zal voor die 3 cijfers 020 hebben. De laatste 2 cijfers zijn controlecijfers die als volgt bepaald worden:

1. als de persoon voor het jaar 2000 geboren is, zijn de laatste 2 cijfers 97 min de rest bij deling door 97 van de eerste 9 cijfers.
2. als de persoon in het jaar 2000 of later geboren is, zijn de laatste 2 cijfers 97 min de rest bij deling door 97 van de eerste 9 cijfers voorafgegaan door een 2.

Als een vrouwelijke professor geboren is op 29 februari 1980, en er 108 vrouwen voor haar geboren werden, wat is dan haar rijksregisternummer?

Het rijksregisternummer is 80 02 29 218 24.

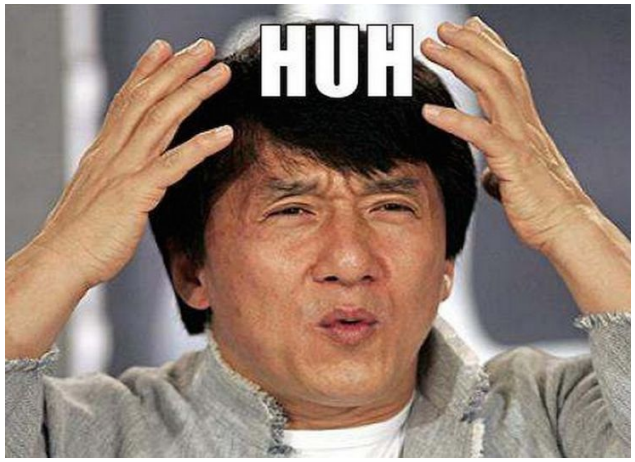
Projectieve vlakken

25 Eindige meetkunde

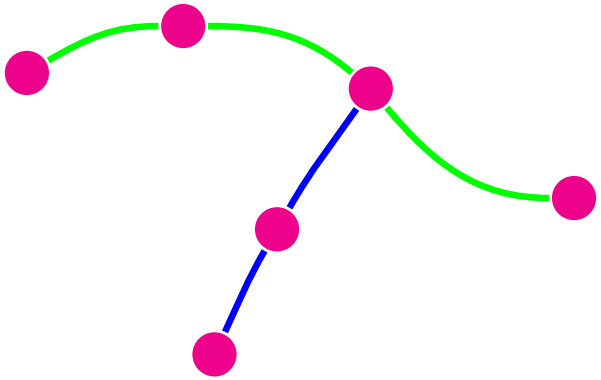
Nood aan een efficiente manier om codes op te stellen

$\Rightarrow$ Oplossing: meetkunde!

26 Eindige meetkunde



- Rechten zijn niet recht
- Rechten hebben een eindig aantal punten



De Fanocode

0000000	1111111
1101000	0010111
0110100	1001011
0011010	1100101
0001101	1110010
1000110	0111001
0100011	1011100
1010001	0101110

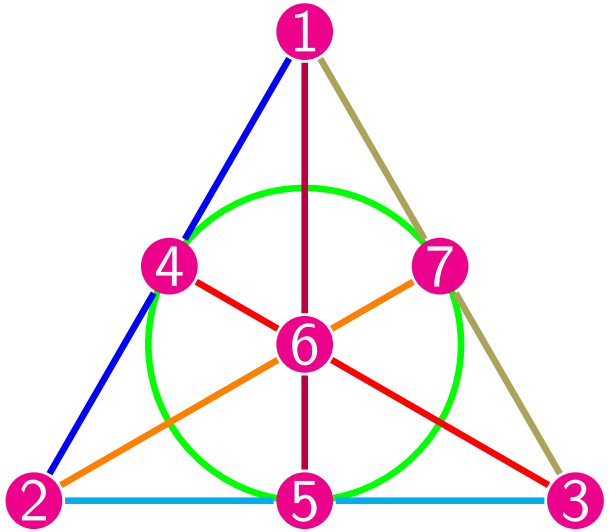
Niet-nul-posities

{1,2,4}	{3,5,6,7}
{2,3,5}	{1,4,6,7}
{3,4,6}	{1,2,5,7}
{4,5,7}	{1,2,3,6}
{1,5,6}	{2,3,4,7}
{2,6,7}	{1,3,4,5}
{1,3,7}	{2,4,5,6}

28 De Fanocode

Probeer 7 stippen te tekenen en te nummeren zodat elk van deze drietallen op een lijn ligt.

{1,2,4}
{2,3,5}
{3,4,6}
{4,5,7}
{1,5,6}
{2,6,7}
{1,3,7}

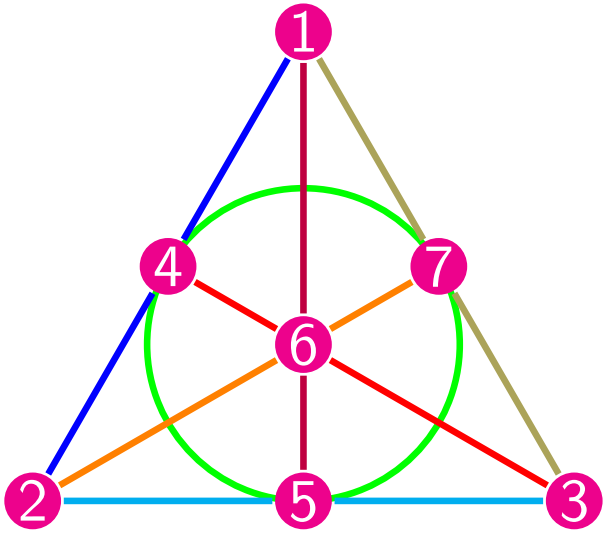


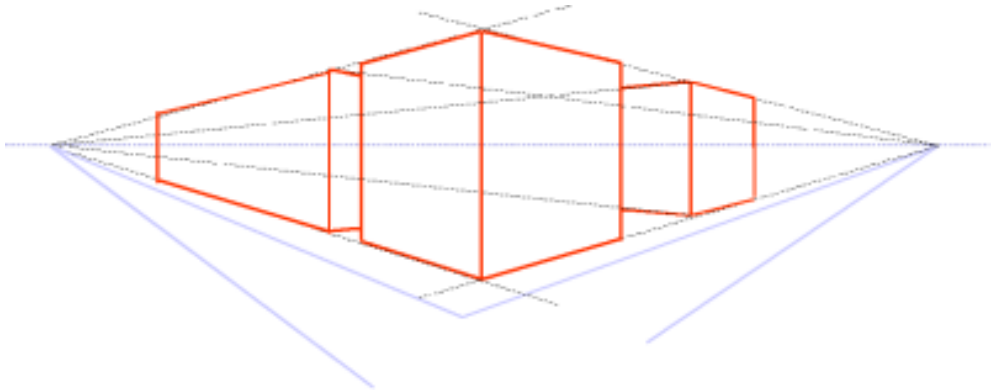
Fanovlak

29 Projectieve Vlakken

Definitie

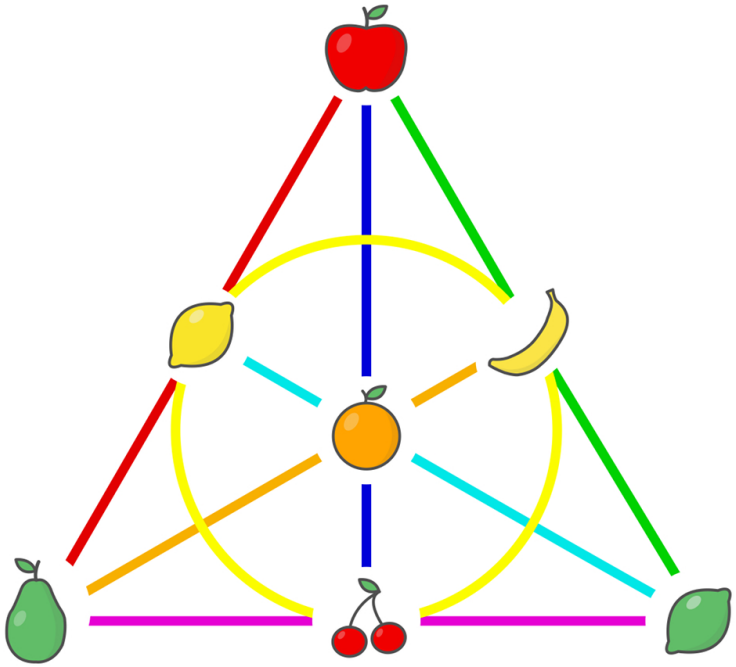
1) Door elke twee punten gaat juist één rechte.
2) Elke twee rechten hebben een punt gemeen.
3) Er bestaat een vierhoek.

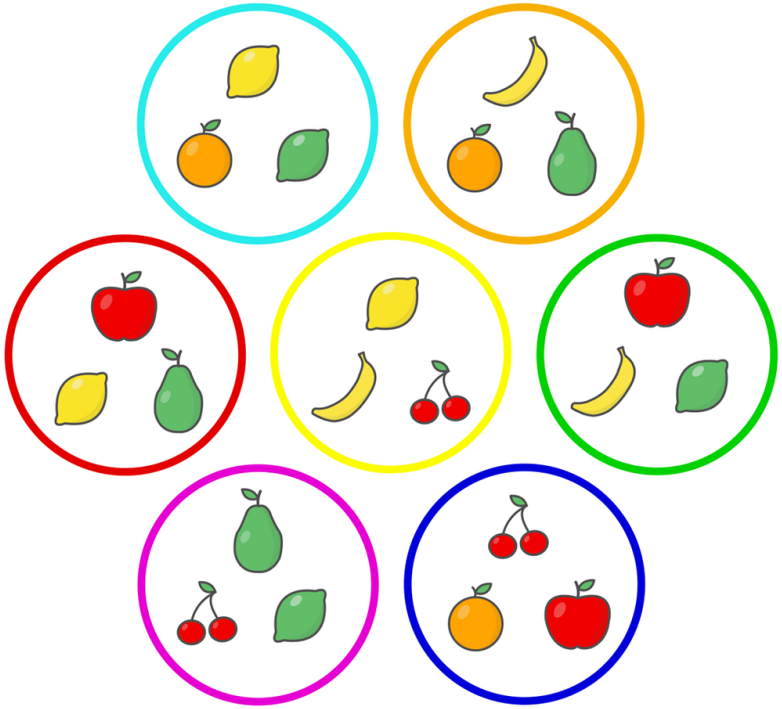




30 Projectieve Vlakken

31 Projectieve Vlakken





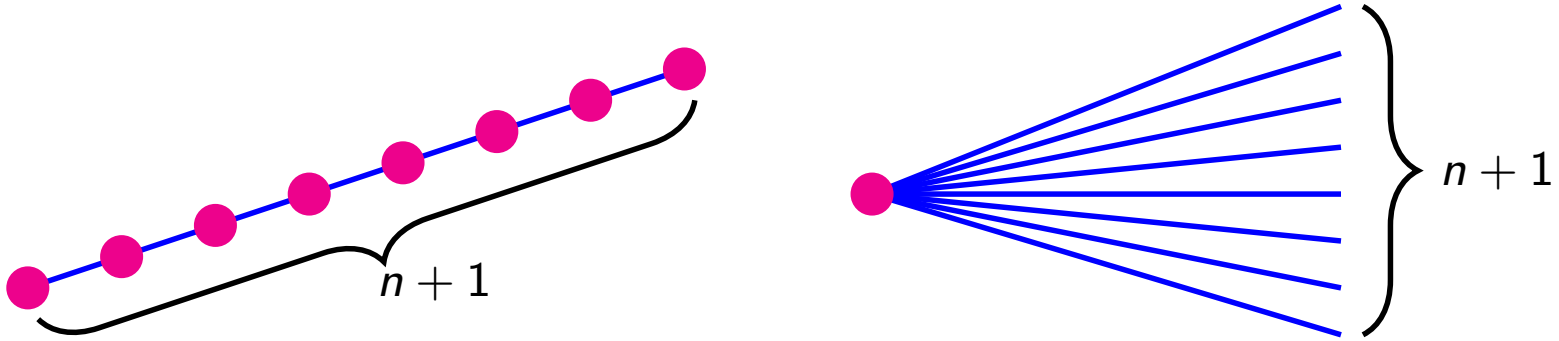
32 Eigenschappen projectief vlak

Definitie

1) Door elke twee punten gaat juist één rechte.
2) Elke twee rechten hebben een punt gemeen.
3) Er bestaat een vierhoek.

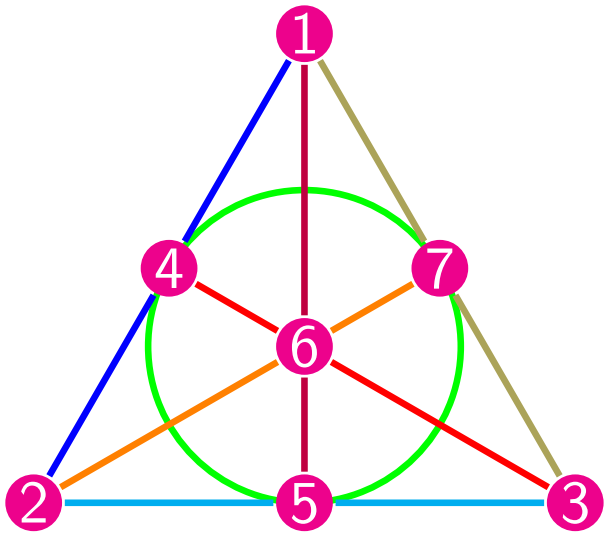
Eigenschap

- Alle rechten hebben hetzelfde aantal punten.
- Door elk punt gaat hetzelfde aantal rechten.



n is de **orde** van het projectief vlak.

33 Projectief vlak van orde $n = 2$



34 Projectief vlak van orde $n = 3$

Teken een projectief vlak van orde 3 met de gegeven $3^2 + 3 + 1 = 13$ punten.

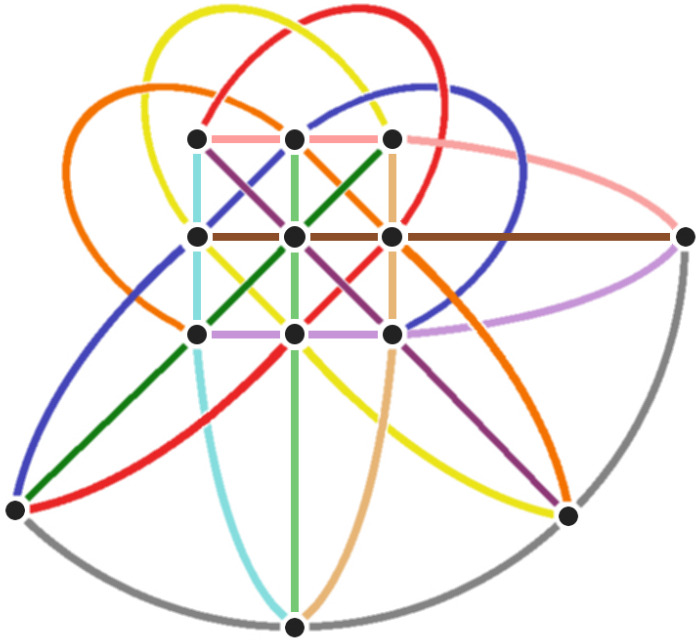
Definitie

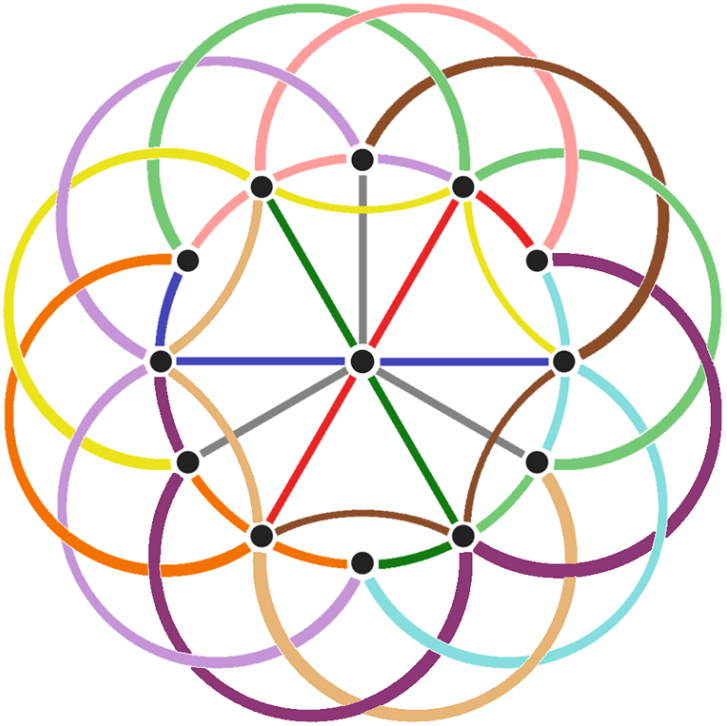
1) Door elke twee punten gaat juist één rechte.
2) Elke twee rechten hebben een punt gemeen.
3) Er bestaat een vierhoek.

Eigenschap

- Alle rechten hebben 4 punten.
- Door elk punt gaan 4 rechten.

35 Projectief vlak orde 3





De Fanocode

0000000	1111111
1101000	0010111
0110100	1001011
0011010	1100101
0001101	1110010
1000110	0111001
0100011	1011100
1010001	0101110

Niet-nul-posities

{1,2,4}	{3,5,6,7}
{2,3,5}	{1,4,6,7}
{3,4,6}	{1,2,5,7}
{4,5,7}	{1,2,3,6}
{1,5,6}	{2,3,4,7}
{2,6,7}	{1,3,4,5}
{1,3,7}	{2,4,5,6}

37 De Fanocode

Elk codewoord met 3 eentjes komt overeen met een rechte van het Fanovlak.

Waarmee komen codewoorden met 4 eentjes overeen in het Fanovlak?

Geef een meetkundig argument waarom de afstand tussen twee codewoorden in de eerste kolom gelijk is aan 4.

Waarom is de afstand tussen een codewoord uit de eerste en één uit de tweede kolom gelijk aan 3 of 7?

38 De Fanocode

De Fanocode is 1-fout verbeterend, en de minimumafstand is 3.
'Echte' codes hebben grotere lengte en verbeteren meer fouten.
Werk bijvoorbeeld met projectieve vlakken van grotere ordes!

Loterij

Een loterijspel bestaat uit het trekken van drie getallen uit de getallen 1 tot 14. Gebruik 2 Fanovlakken (één genummerd van 1 tot 7 en één van 8 tot 14) om 14 loten op te stellen zodat er zeker een lot is met 2 winnende getallen.

Golf

Zeven golfers willen op zeven verschillende dagen telkens in twee groepen (één van 3 en één van 4) tegen mekaar spelen. Hoe kunnen ze dat doen als ieder persoon met ieder andere een gelijk aantal keren in de groep wil vertoeven?
Kan je dezelfde vraag oplossen voor acht golfers, zeven dagen en twee groepen van 4?

Latijnse vierkanten

41 Latijnse vierkanten

Op elke rij en elke kolom komt elk symbool uit $\{a, b, c\}$ juist één keer voor.

Voorbeeld

a	b	c
b	c	a
c	a	b

Het aantal rijen (kolommen) is de *orde* n van het Latijns vierkant.

Latijnse Vierkanten

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

43 Grieks-Latijnse vierkanten

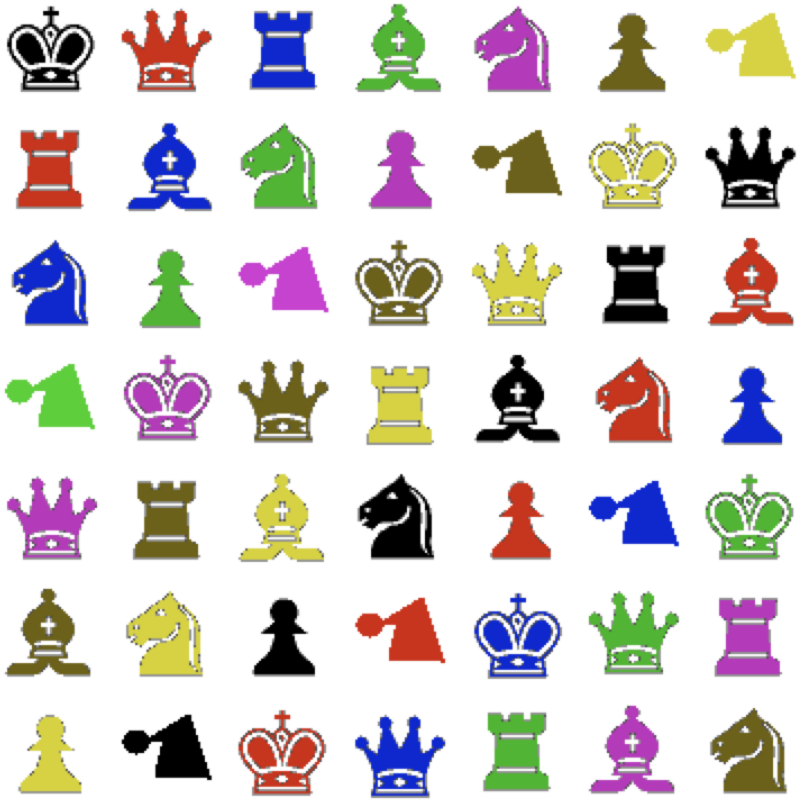
Op elke rij en elke kolom komt elke letter uit $\{a, b, c\}$ en elke letter uit $\{\alpha, \beta, \gamma\}$ juist één keer voor.
In totaal komt elk koppel uit $\{a\alpha, a\beta, a\gamma, b\alpha, b\beta, b\gamma, c\alpha, c\beta, c\gamma\}$ juist één keer voor.

Voorbeeld

aα	bβ	cγ
bγ	cα	aβ
cβ	aγ	bα

Grieks-Latijnse vierkanten

45 Grieks-Latijnse vierkanten



46 Grieks-Latijnse vierkanten

Maak een Grieks-Latijns vierkant van orde 4

Leg de speelkaarten met cijfers uit $\{1, 2, 3, 4\}$ in een 4x4 rooster zodat op elke rij en elke kolom elk cijfer en elk symbool juist één keer voorkomt.

1
2
3
4
2
3
4
1
3
4
1
2
4
1
2
3
3
4
1
2

48 Grieks-Latijnse vierkanten

36 officieren

6 van elke rang en 6 van elk regiment.
Plaats deze zodat op elke rij en kolom er juist 1 officier met elke rang en regiment voorkomt.

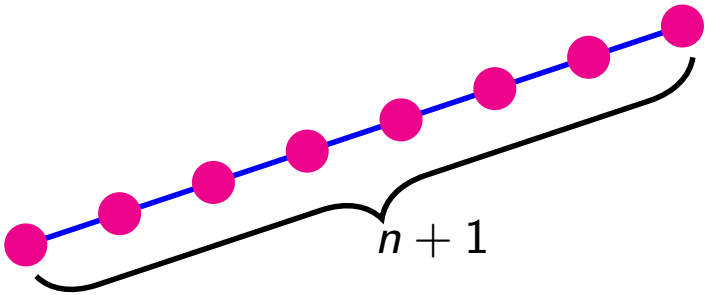
Grieks-Latijnse vierkanten

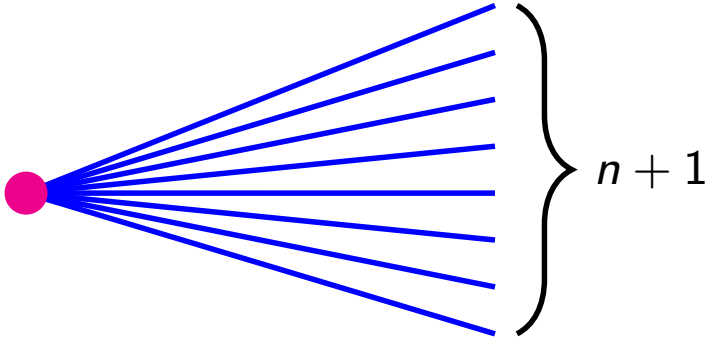
- Euler: lukt steeds als n oneven is of als n een veelvoud is van 4
- Vermoeden van Euler: lukt niet als n gelijk is aan een viervoud plus twee (2,6,10,14,...).
- Voor orde 6 lukt dit nooit! (Tarry, 1901)
- 1959: Bose, Parker, Shrikhande: lukt voor alle $n \geq 10$.

Grieks-Latijnse vierkanten

Eigenschap

- Alle rechten hebben hetzelfde aantal punten.
- Door elk punt gaat hetzelfde aantal rechten.



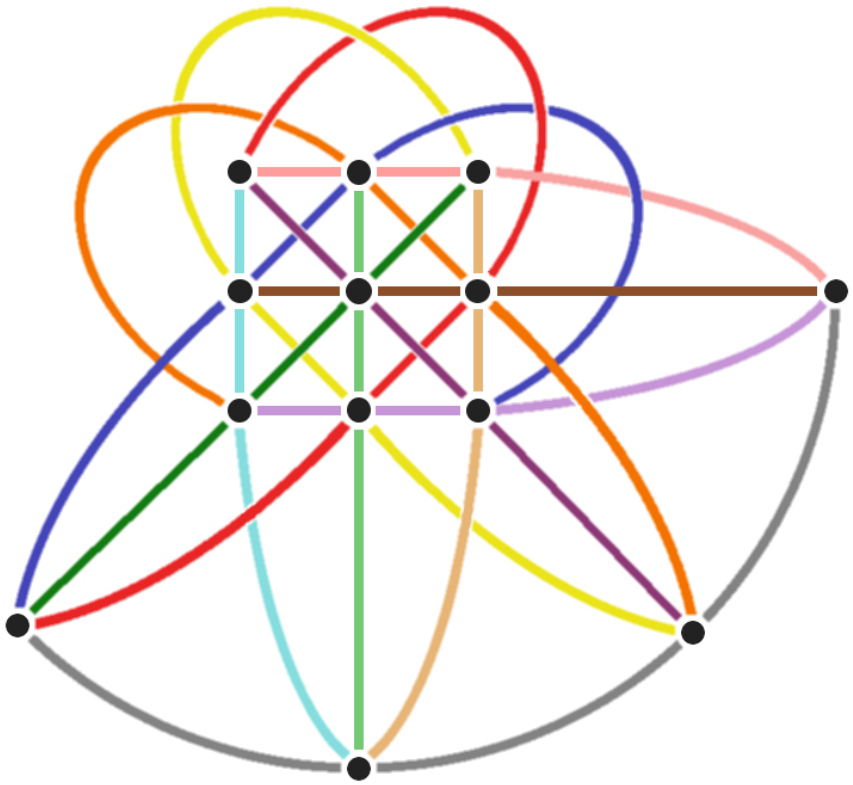


n is de **orde** van het projectief vlak.

Als een projectief vlak van orde $n > 2$ bestaat, dan bestaat ook een Grieks-Latijns vierkant van orde n.

51 Voorbeeld

Dit projectief vlak van orde 3 geeft aanleiding tot een Grieks-Latijns vierkant van orde 3 en omgekeerd.



Projectieve vlakken

- Welke ordes van een projectief zijn mogelijk?
- $n = 6$ zeker niet (via Latijnse vierkanten)

- Voor elke priemmacht $q = p^h$, p priem, bestaat er een projectief vlak van orde q

Priemmachtvermoeden

De orde van een projectief vlak is altijd een priemmacht.

That's all Folks!
SUWALLS

UNIVERSITEIT GENT

Campus Sterre

Krijgslaan 281, 9000 Gent

Huisnummer

Ingang rolstoeltoegankelijk

Fietsenstalling

Resto