WHY DO WE NEED MATH?

FINDING X IS ONLY USEFUL IF YOU'RE A PIRATE

Mis on “Matemaatika”

Milleks seda õpetatakse?

1. Matemaatika on teadmiste kogum

Hulgateooria

Mat. loogika

Analüüs

Algebra

Disk.mat

Fn. analüüs, Tõenäosusteooria ja statistika, Optimiseerimine, Geomeetria, Krüptograafia, …

Omadused, algoritmid, rakendused.

2. Matemaatika on abstraktsiooni oskus

$2 + 3 \cdot 4$

$(\mathbb{R}, +, \times)$: $a + c \times b$

Rühm/Ring/Korpus/Ruum

Algebrad

Algebralised struktuurid

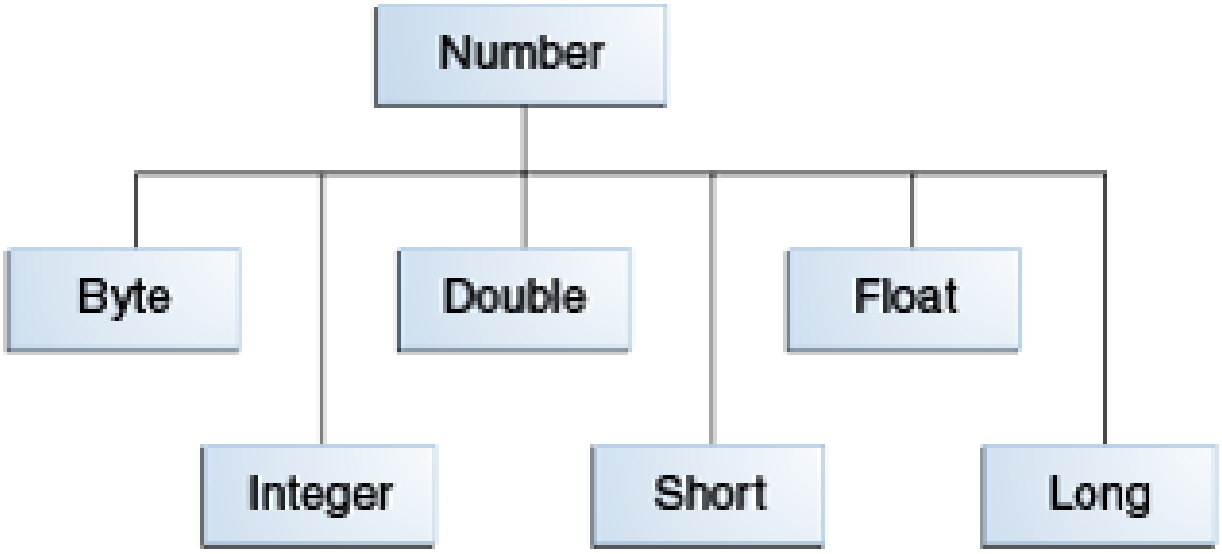
2. Abstraktsiooni oskus

```
class RealNumber {
      operator + (RealNumber a, RealNumber b);
      operator * (RealNumber a, RealNumber b);
}
```

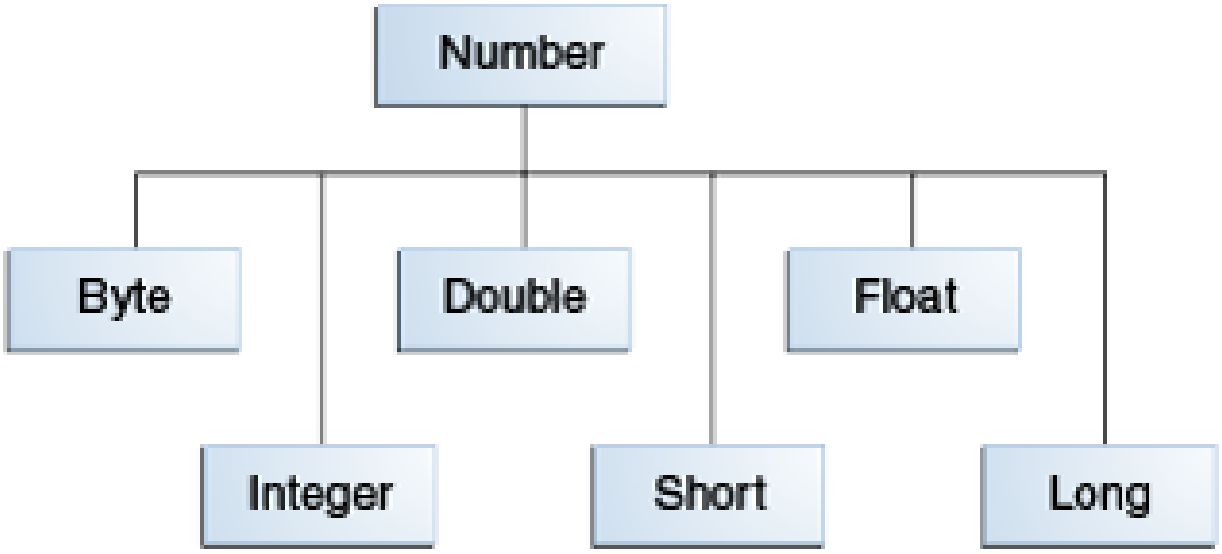
2. Abstraktsiooni oskus

```
class RealNumber implements FieldElement {
      operator + (RealNumber a, RealNumber b);
      operator * (RealNumber a, RealNumber b);
}

interface FieldElement {
      operator + (FieldElement a, FieldElement b);
      operator * (FieldElement a, FieldElement b);

      constraint
       [FieldElement a,b,c => a*(b+c) = a*b + a*c]
}
```

2. Abstraktsiooni oskus

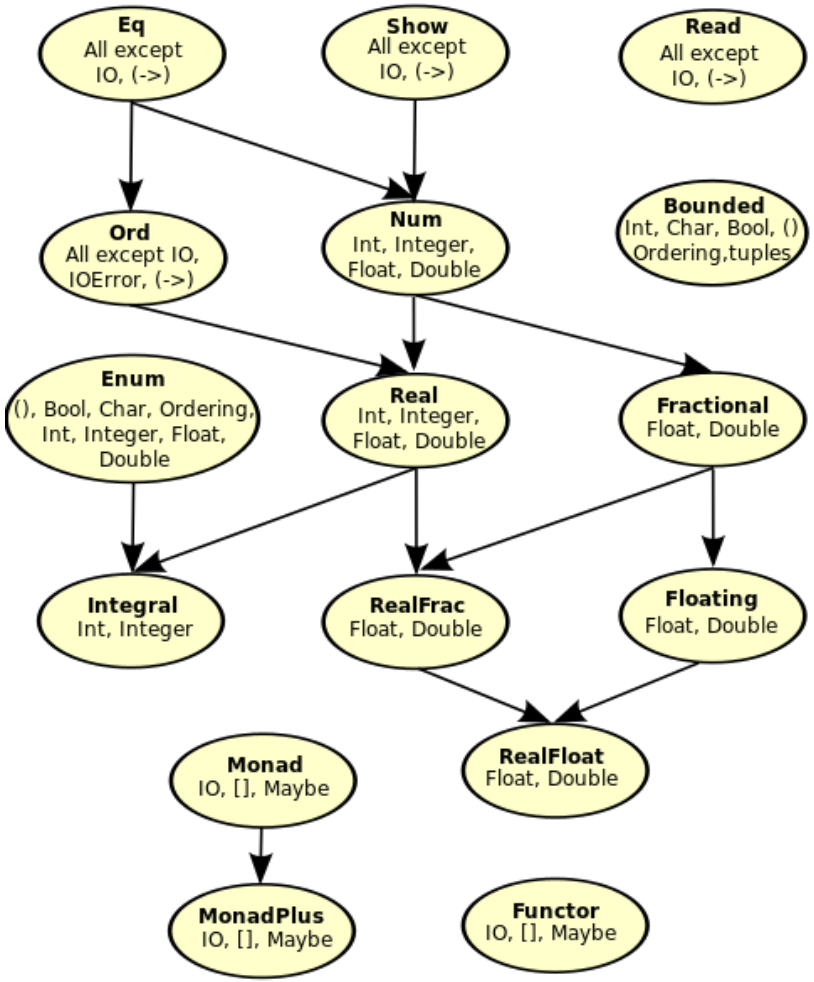


2. Abstraktsiooni oskus

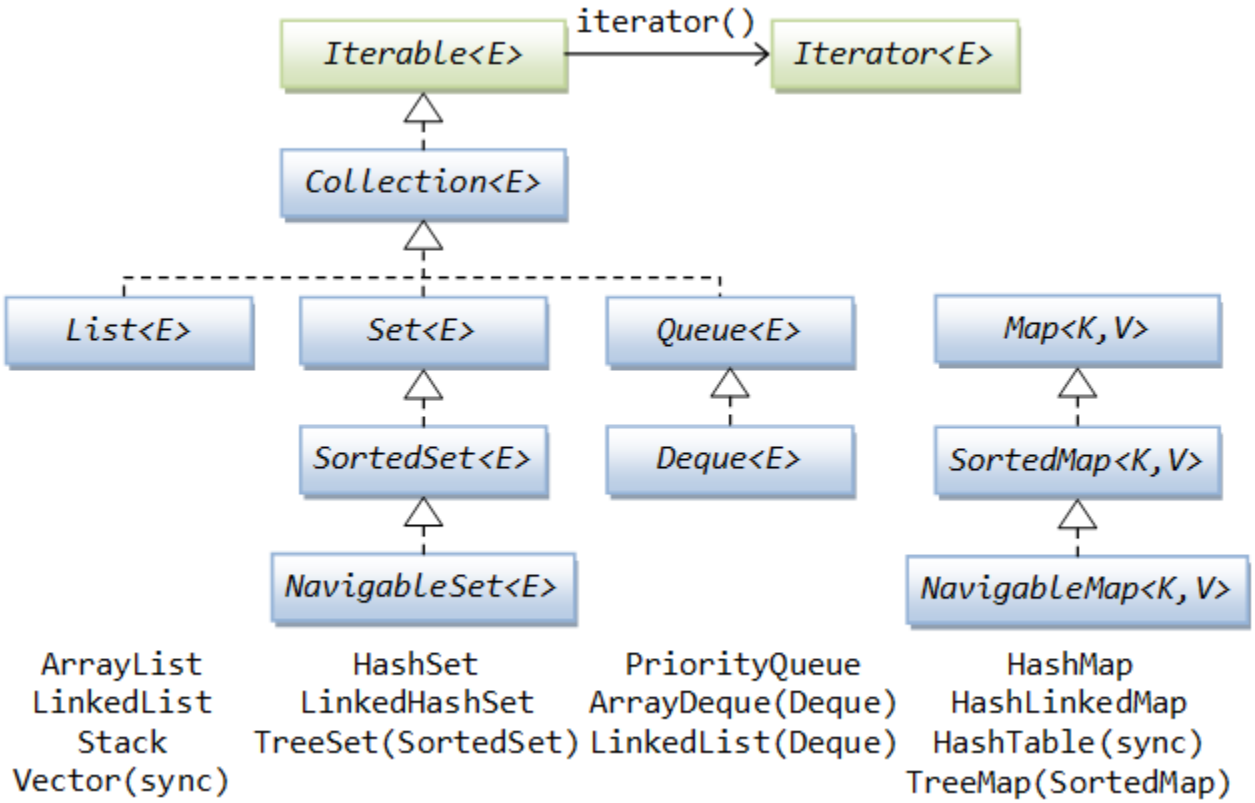


BigDecimal?
Fractional?
Complex?
Interval?
Vector?
Matrix?
Polynomial?

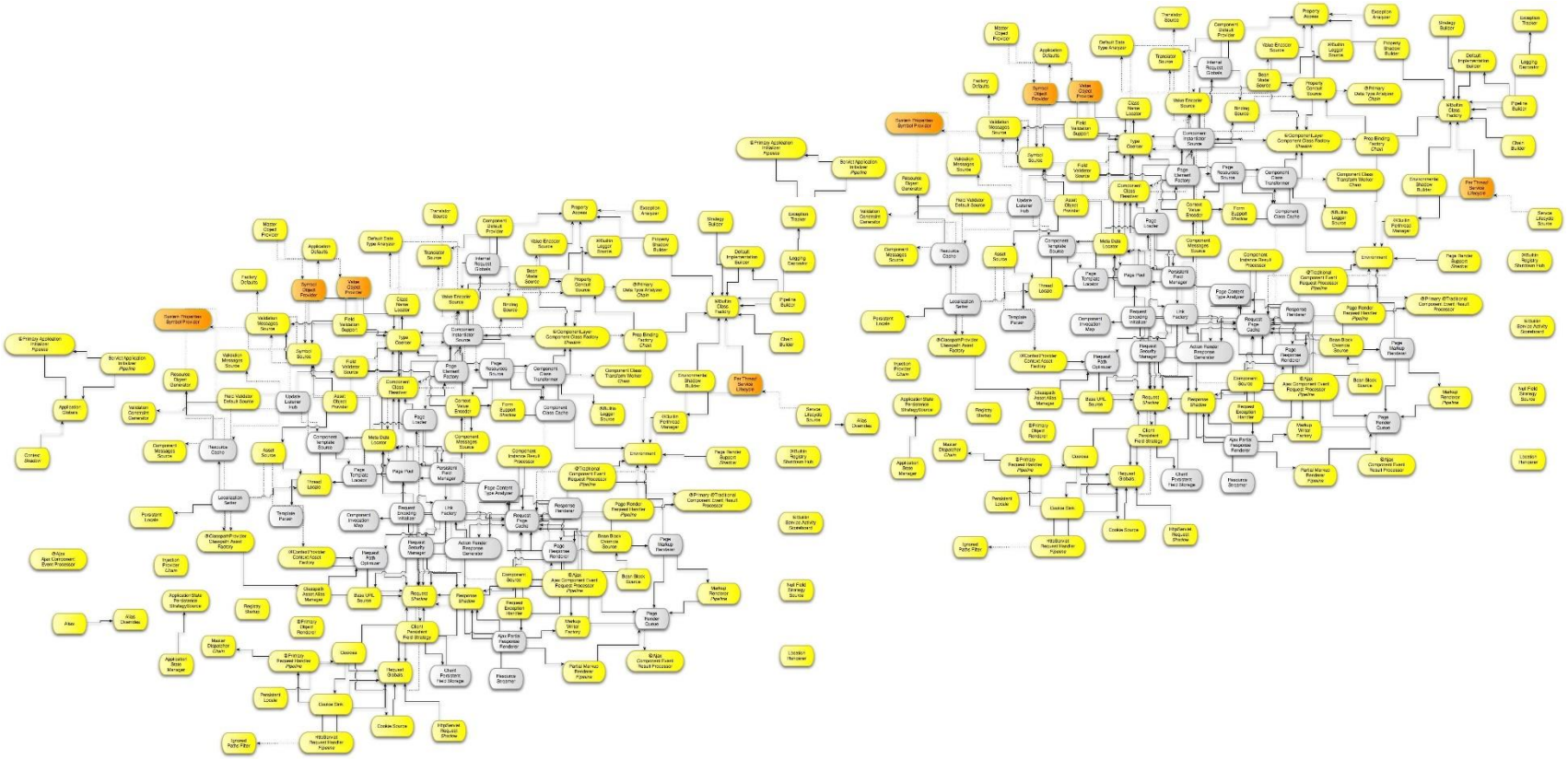
2. Abstraktsiooni oskus



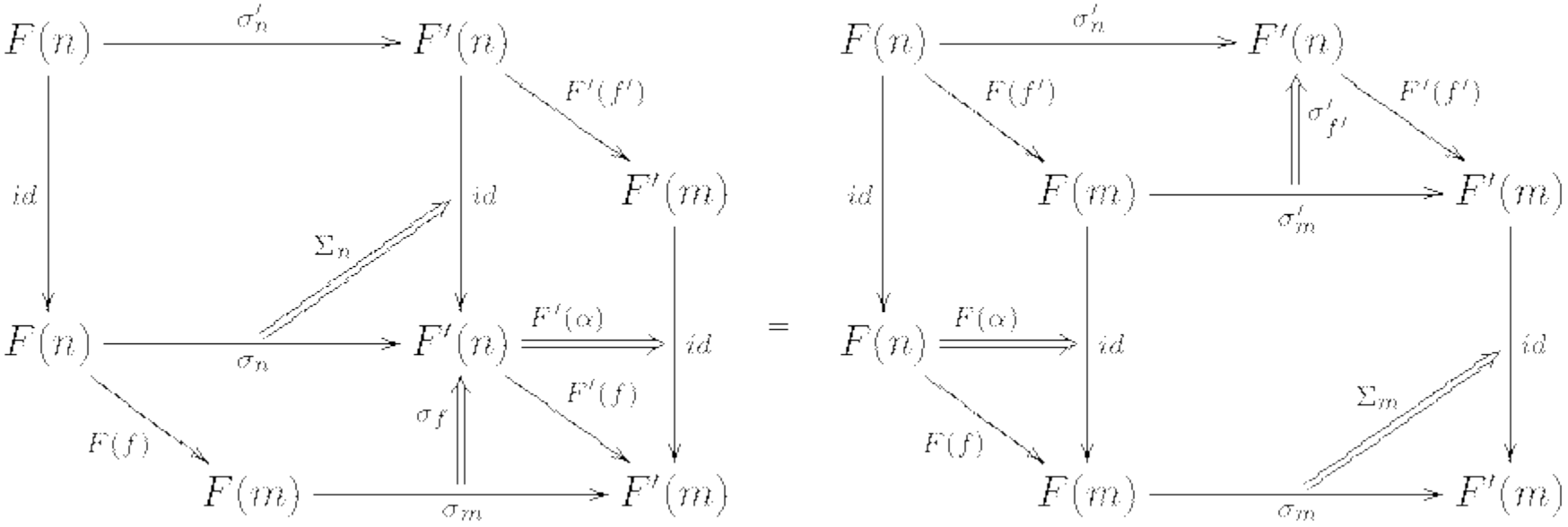
2. Abstraktsiooni oskus



2. Abstraktsiooni oskus



2. Abstraktsiooni oskus

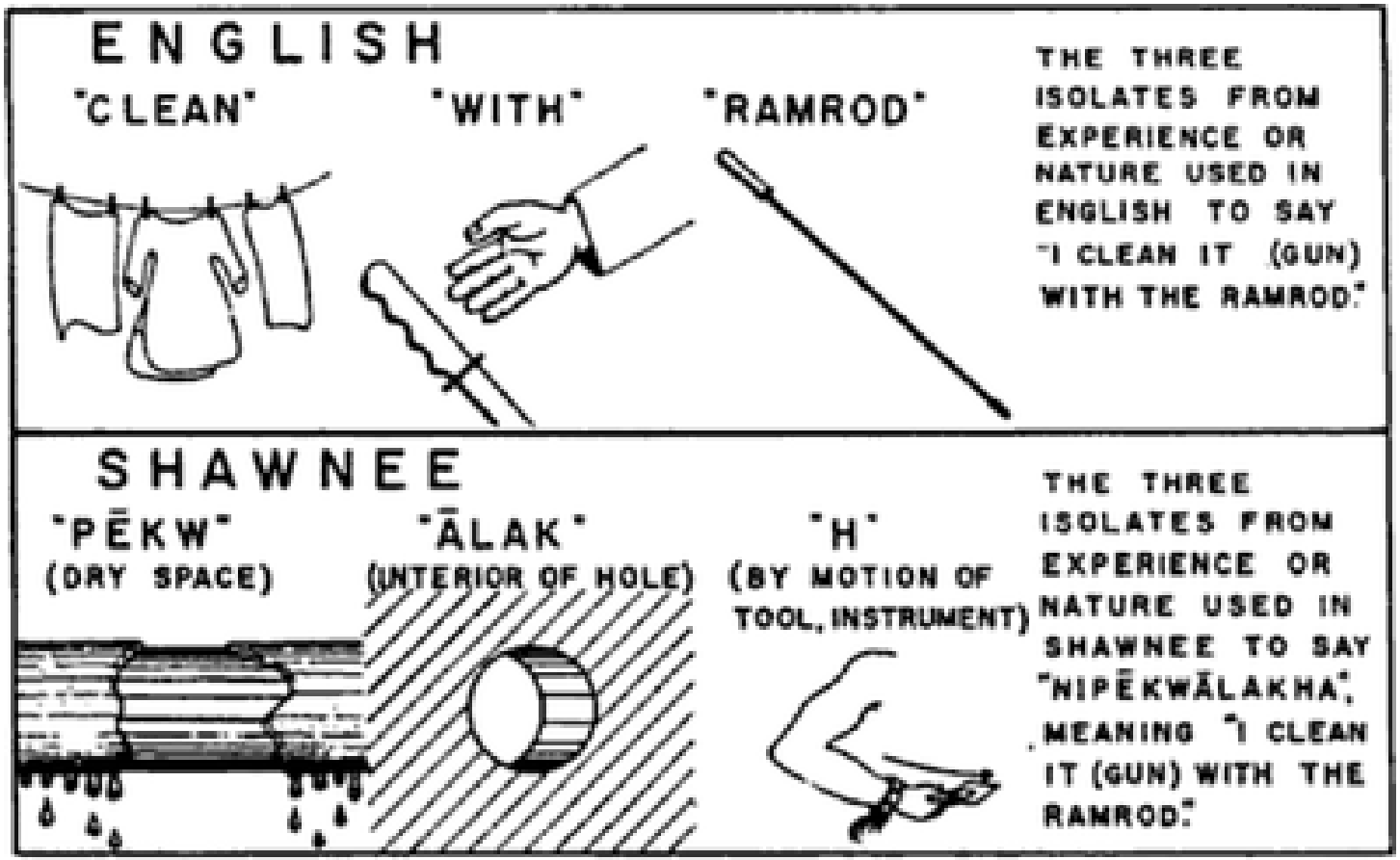


Keel

Keel

Keel

"Keeleline relativism"


ENGLISH
"CLEAN"
"WITH"
"RAMROD"
THE THREE ISOLATES FROM EXPERIENCE OR NATURE USED IN ENGLISH TO SAY "I CLEAN IT (GUN) WITH THE RAMROD."
SHAWNEE
"PĒKW"
(DRY SPACE)
"ĀLAK"
(INTERIOR OF HOLE)
"H"
(BY MOTION OF TOOL, INSTRUMENT)
THE THREE ISOLATES FROM EXPERIENCE OR NATURE USED IN SHAWNEE TO SAY "NIPĒKWĀLAKHA", MEANING "I CLEAN IT (GUN) WITH THE RAMROD."

1. Matemaatika on teadmiste kogum

Hulgateooria

Mat. loogika

Analüüs

Algebra

Disk.mat

Fn. analüüs, Tõenäosusteooria ja statistika, Optimiseerimine, Geomeetria, Krüptograafia, …

Omadused, algoritmid, rakendused.

Füüsika

And God Said

$$\nabla \cdot \vec{D} = \rho_{\text{free}}$$

$$\nabla \cdot \vec{B} = 0$$

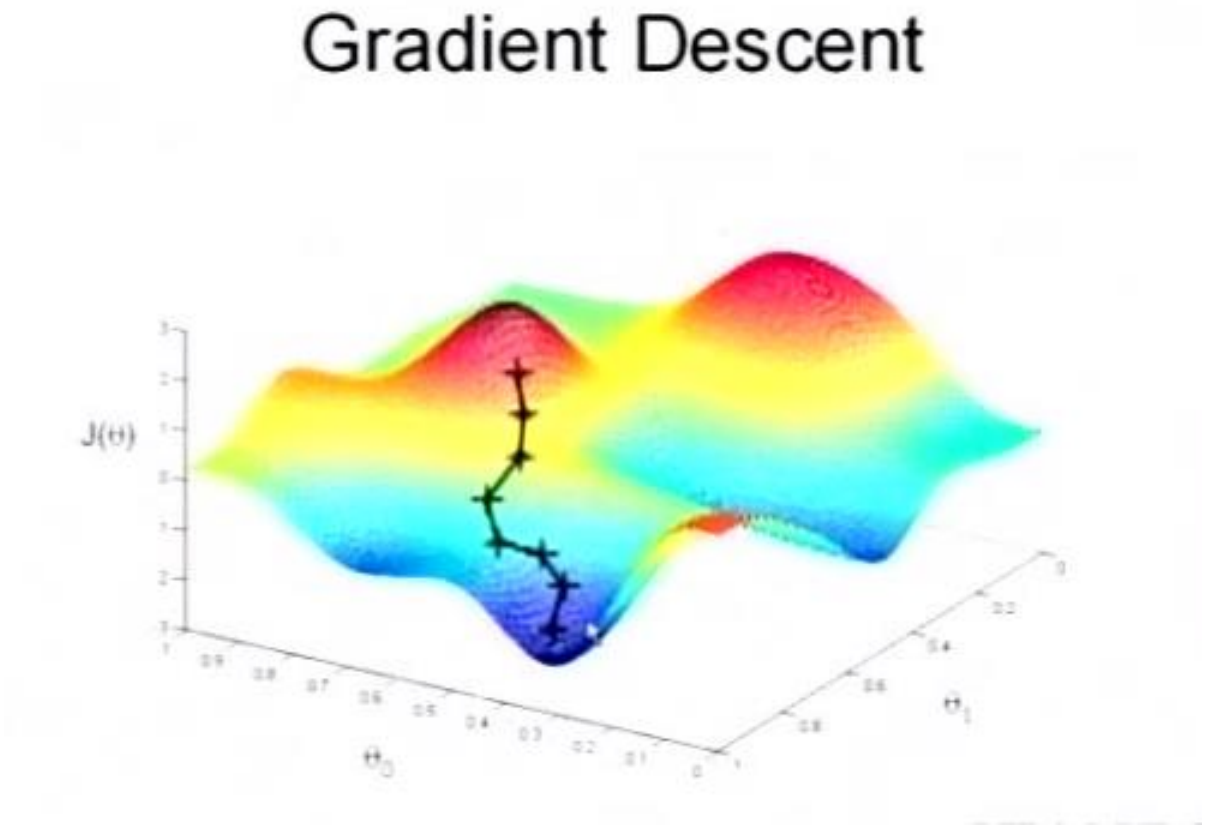
$$\nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}$$

$$\nabla \times \vec{H} = \vec{J}_{\text{free}} + \frac{\partial \vec{D}}{\partial t}$$

and *then* there was light.

Tõenäosusteooria

Optimiseerimine



1. Matemaatika on teadmiste kogum

Hulgateooria

Mat. loogika

Analüüs

Algebra

Disk.mat

Fn. analüüs, Tõenäosusteooria ja statistika, Optimiseerimine, Geomeetria, Krüptograafia, …

Omadused, algoritmid, rakendused.

Algebralised teisendused

- $\big(a \times (b + a)\big) \to a \times b + a \times a \to a \times b + a$

Algebralised teisendused

- $\big(a \times (b + a)\big) \to a \times b + a \times a \to a \times b + a$

- Näiteks, optimiseeriv kompileerimine

Algebralised teisendused

```
select id from users, permissions, page
where users.id             = permissions.user_id and
      permissions.page_id = page.id              and
      permissions.type     = 'read'
```

Algebralised teisendused

```
select id from users, permissions, page
where users.id             = permissions.user_id and
      permissions.page_id  = page.id             and
      permissions.type     = 'read'
```

$$\pi_{U.id} \cdot \sigma_{P} \cdot \sigma_{P,\Pi} \cdot \sigma_{U,P}(U \times P \times \Pi)$$

Algebralised teisendused

```
select id from users, permissions, page
where users.id            = permissions.user_id and
      permissions.page_id = page.id             and
      permissions.type    = 'read'
```

$$\pi_{U.id} \cdot \sigma_P \cdot \sigma_{P,\Pi} \cdot \sigma_{U,P}(U \times P \times \Pi) \rightarrow$$
$$\pi_{U.id} \cdot \sigma_{P,\Pi} \cdot \sigma_{U,P} \cdot \sigma_P(U \times P \times \Pi) \rightarrow$$
$$\sigma_{P,\Pi}(\sigma_{U,P}(\pi_{U.id}(U) \times \sigma_P(P)) \times \Pi)$$

or

$$\sigma_{U,P}(\pi_{U.id}(U) \times \sigma_{P,\Pi}(\sigma_P(P) \times \Pi))$$

Enimkasutatavad algebralised struktuurid

- Vektorruum $\mathbb{R}^n$ või $\mathbb{C}^n$
- Lineaarteisenduste/Maatriksite ring $\mathbb{R}^{m\times n}$
- Ring/Korpus $\mathbb{Z}_n$
- Ring $\mathbb{F}[x]$

Enimkasutatavad algebralised struktuurid

- Vektorruum $\mathbb{R}^n$ või $\mathbb{C}^n$
- Lineaarteisenduste/Maatriksite ring $\mathbb{R}^{m\times n}$
- Ring/Korpus $\mathbb{Z}_n$
- Ring $\mathbb{F}[x]$

Lineaaralgebra

- Vektorruum $\mathbb{R}^n$ või $\mathbb{C}^n$
- Lineaarteisenduste/Maatriksite ring $\mathbb{R}^{m\times n}$

Lineaaralgebra

- $\mathbb{R}^n$ või $\mathbb{C}^n$

Lineaaralgebra

- $\mathbb{R}^n$ või $\mathbb{C}^n$
  - Punkt või suund kahe- või kolmemõõtmelises ruumis
  - Objekti karakteristikute komplekt
  - Signaal (heli, pilt, video)
  - Objekti "kood"

- $\mathbb{R}^{m \times n}$
  - Graafi seosed
  - Tõenäosusjaotus(ed)

Diskreetne matemaatika

- Vektorruum $\mathbb{R}^n$ või $\mathbb{C}^n$
- Lineaarteisenduste/Maatriksite ring $\mathbb{R}^{m\times n}$
- Ring/Korpus $\mathbb{Z}_n$
- Ring $\mathbb{F}[x]$

Diskreetne matemaatika

- Arvuti jaoks kõige tähtsam korpus?

Diskreetne matemaatika

- Arvuti jaoks kõige tähtsam korpus?
  - $(\mathbb{Z}_2, +, \times)$

Diskreetne matemaatika

- Arvuti jaoks kõige tähtsam korpus?
  - $(\mathbb{Z}_2, +, \times)$
  - $(\mathbb{Z}_{2^n}, +, \times)$

Diskreetne matemaatika

- Arvuti jaoks kõige tähtsam korpus?
  - $(\mathbb{Z}_2, +, \times)$
  - $(\mathbb{Z}_{2^n}, +, \times)$
  - $(\mathbb{Z}_{2^n}, +_F, \times_F)$

Diskreetne matemaatika

- Arvuti jaoks kõige tähtsam korpus?
  - $(\mathbb{Z}_2, +, \times)$
  - $(\mathbb{Z}_{2^n}, +, \times)$
  - $(\mathbb{Z}_{2^n}, +_F, \times_F) \sim ? (\mathbb{R}, +, \times)$

Diskreetne matemaatika

- Krüptograafia
  - $(\mathbb{Z}_n, \times)$
  - Olgu $g \in \mathbb{Z}_n$, siis $G = \{g^a : a \in \mathbb{Z}_n\}$ on $(\mathbb{Z}_n, \times)$ alamrühm.
    - Diskreetne logarithm, Diffie-Hellman
    - G suurus, RSA

Kokkuvõte

- Matemaatika on abstraktsioonivõime.
- Seda on ka praktikas vaja
- Igal pool
- Võtke seda tõsiselt