Arithmetische Komplexität

Polynome & Schaltkreise

Julian Lorenz

February 9, 2021

Goethe University

Polynome

Berechnung:	
von	Polynomen $f \in \mathbb{F}[x_1, x_2, \cdots]$
durch	Arithmetische Schaltkreise

- Beliebiger Körper $\mathbb{F}$ mit Charakteristik 0

$\rightarrow$ min $k \in \mathbb{N}\backslash\{0\} : k \cdot \mathit{neutral}(\times) = \mathit{neutral}(+)$

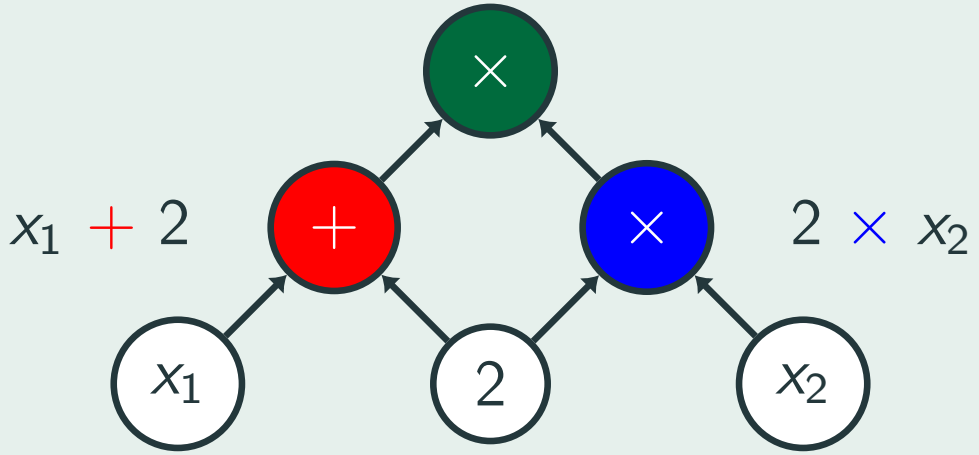
- Grad d von f ist polynomiell in n
- Multilinear: d durch Anzahl der Variablen beschränkt

$\rightarrow$ Größtmögliches Monom: $x_1 \cdot x_2 \cdot \ldots \cdot x_{n-1} \cdot x_n$

Arithmetische Schaltkreise

- Entsprechen gerichteten kreisfreien Graphen $G(V, E)$
- Knoten / Gatter mit Eingangsgrad 0 sind Polynome
- Alle anderen Knoten / Gatter entsprechen $+$ oder $\times$
- **Arithmetische Formel:** $\forall V \in G$: Ausgangsgrad $= 1$
- **Größe:** Anzahl der Kanten (oder Knoten) von G

$$f(x_1, x_2) = ((x_1 + 2) \times (2 \times x_2)) = 2x_1x_2 + 4x_2$$



Größe von Schaltkreisen

Definition

$\mathrm{S}(f)$ ist die minimale Größe eines arithmetischen Schaltkreises, der f berechnet. $\mathrm{L}(f)$ ist die minimale Größe einer arithmetischen Formel, die f berechnet.

$\Rightarrow$ Es gilt $\mathrm{S}(f) \leq \mathrm{L}(f)$

- Sei $p(x) \in \mathbb{F}(x)$ ein univariates Polynom vom Grad d

Horner's Rule:

$$p(x) = \sum_{i=0}^{d} a_i x^i = a_0 + x(a_1 + \cdots + x(a_{d-1} + x a_d) \cdots)$$

- d Additionen & d Multiplikationen $\Rightarrow S(f) = \mathcal{O}(d)$

Einfache univariate Polynome

Polynom $g(x) = x^d$, $d \in \mathbb{N}$

Ausgabegatter

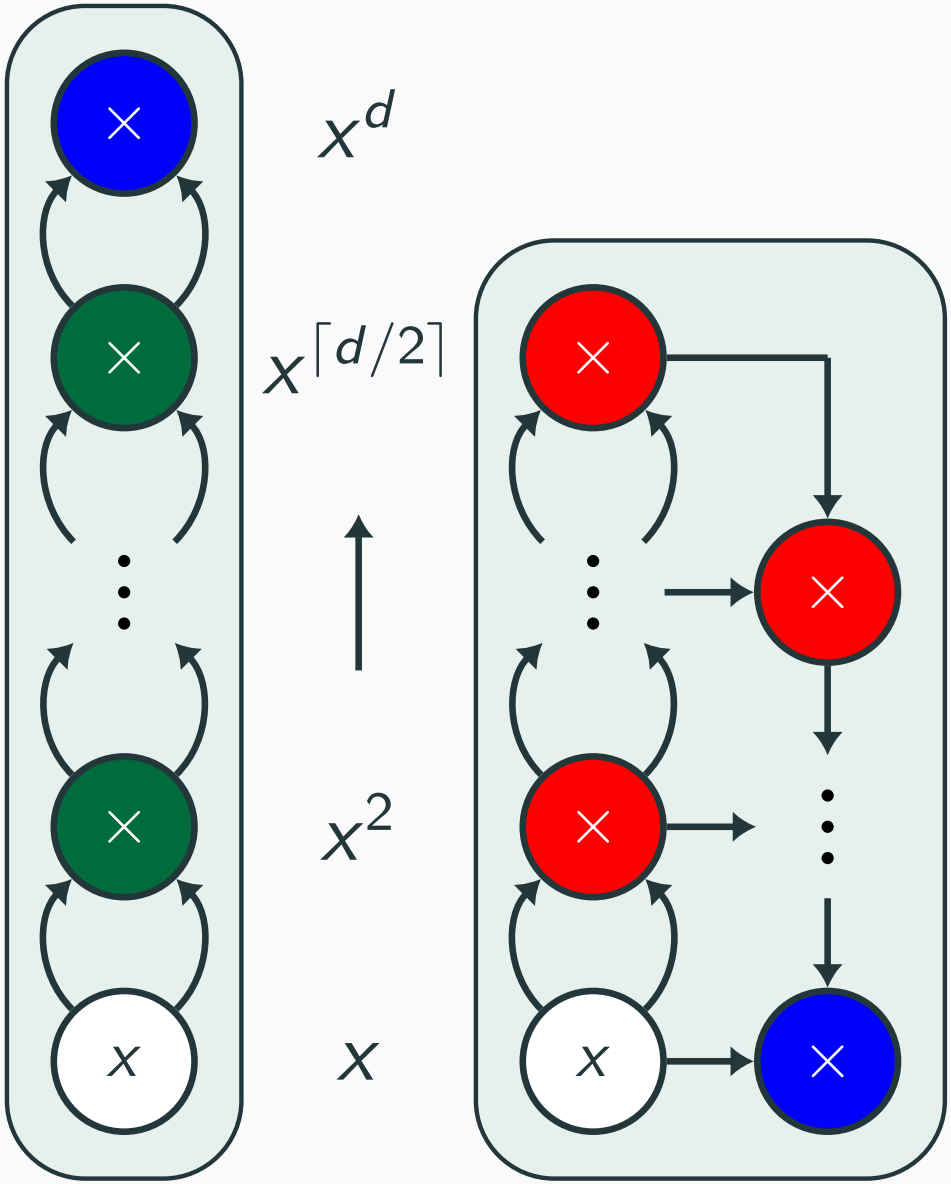
Best Case: $d = 2^n$, $n \in \mathbb{N}$

Worst Case: $d = 2^n - 1$

$\Rightarrow S(g) = \Theta(\log(d))$

- Vielfache Nullstelle
- $x^2 = x$ für $\mathbb{F}_2$ ↯

$\Leftrightarrow x^2 - x = 0 \neq$ Nullpolyom



Schwere univariate Polynome

- **Idee:** Polynom $h(x)$ mit d unterschiedlichen Nullstellen

$\Rightarrow$ $h(x) = (x-1) \cdot (x-2) \cdot \ldots \cdot (x-(d-1)) \cdot (x-d)$

- Nur das offensichtliche $\log(d) \leq S(h) \leq d$ bekannt!
- **Offene Frage:** Grad d Polynom mit $\mathrm{S}(f) \neq \mathcal{O}(\log(d))$

Theorem

Falls $S(h) \leq (\log(d))^{\mathcal{O}(1)}$ ist Integer Factoring in $\mathcal{P}/poly$.

Erinnerung: $\mathcal{P}/\mathrm{poly}$ ist die Menge aller Funktionen $f : \mathbb{I} \to \mathbb{I}$, die von einer Familie von Schaltkreisen polynomieller Größe berechnet werden kann.

Symmetrische Polynome

Definition

$p(x_1, \cdots, x_n)$ ist ein *symmetrisches Polynom* genau dann, wenn man zwei beliebige x_i, x_j, $i \neq j$ miteinander vertauschen kann, ohne das Polynom zu verändern.

- **Elementare symmetrische Polynome** als Bausteine:

$$SYM_n^k(x_1, \cdots, x_n) = \sum_{\mathcal{S} \subset [n] : |\mathcal{S}| = k} \prod_{i \in \mathcal{S}} x_i$$

$\rightarrow$ Summe von dem Produkt aller Variablen aller Teilmengen

- Einzigartig für Grad d in n Variablen

Beispiel: Elementares symmetrisches Polynom

$$SYM_n^k(x_1, \cdots, x_n) = \sum_{\mathcal{S} \subset [n] : |\mathcal{S}| = k} \prod_{i \in \mathcal{S}} x_i$$

$n = 4,\ S = \{x_1, x_2, x_3, x_4\}$	
k	SYM_n^k
$k = 1$	$x_1 + x_2 + x_3 + x_4$
$k = 2$	$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$
$k = 3$	$x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$

- $|SYM_n^k(x_1, \cdots, x_n)| = \binom{n}{k}$
- Exponentielle Komplexität

Komplexität: Binomialkoeffizient

- **Stirling Approximation:** $n! \approx \sqrt{2\pi n}(n/e)^n$
- Worst-Case für Binomialkoeffizient: $\binom{2n}{n}$

$$
\begin{aligned}
\binom{2n}{n} &= \frac{(2n)!}{(n!)\cdot(2n-n)!} = \frac{(2n)!}{(n!)^2} \\
(2n)! &\approx 2\sqrt{\pi n}\frac{(2n)^{2n}}{e^{2n}} \\
(n!)^2 &\approx 2\pi n\frac{n^{2n}}{e^{2n}} \\
\binom{2n}{n} &\approx \frac{2\sqrt{\pi n}}{2\pi n} \cdot \frac{e^{2n}}{n^{2n}} \cdot \frac{(2n)^{2n}}{e^{2n}} \\
&= \frac{2^{2n}}{\sqrt{\pi n}}
\end{aligned}
$$

$\Rightarrow$ Komplexität von $\mathcal{O}(\frac{2^n}{\sqrt{n}})$.

Symmetrische Polynome

Symmetrische Polynome sind die *Koeffizienten* des univariaten Polynoms $g(t) = \prod_{i=1}^{n}(t - x_i)$ in einer neuen Variable t.

$$\begin{aligned} g(t) &= t^3 + a_2 t^2 + a_1 t + a_0 \\ &\Leftrightarrow (t - x_1) \cdot (t - x_2) \cdot (t - x_3) \end{aligned}$$

$$\begin{aligned} a_2 &= -x_1 - x_2 - x_3 \\ a_1 &= x_1 x_2 + x_1 x_3 + x_2 x_3 \\ a_0 &= -x_1 x_2 x_3 \end{aligned}$$

- Lineare Interpolation von $n + 1$ unterschiedlichen t

$\Rightarrow$ **Sum-Product-Sum:** $\sum \prod \sum$

Theorem

Für alle n, k gilt $L(f) \leq \mathcal{O}(n^2)$.

Matrix Multiplikation

$C = AB$, $A \in \mathbb{K}^{m \times n}$, $B \in \mathbb{K}^{n \times p}$, $C \in \mathbb{K}^{m \times p}$ mit $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$

Pseudocode:

```
C = [[ 0 for _ in range(p)] for _ in range(m)]
for i in range(m):
    for j in range(p):
        for k in range(n):
            C[ i ][ j ] += A[ i ][ k ] * B[ k ][ j ]
```

$\Rightarrow \mathcal{O}(m \cdot n \cdot p)$ bzw für quadratische Matrizen $\mathcal{O}(n^3)$

Divide & Conquer

$$C = AB,\ A, B, C \in \mathbb{K}^{m \times m} \text{ mit } m = 2^n,\ n \in \mathbb{N}$$

$$C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} \quad A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \quad B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

$$C = \left(\begin{array}{c|c} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ \hline A_{21}B_{11} + A_{21}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{array}\right)$$

- 8 Multiplikationen
- Teilmatrizen der Größe $n/2$
- $\Theta(n^2)$ elementweise Addition

Rekursionsgleichung:

$$T(n) = a \cdot T(\tfrac{n}{b}) + f(n)$$

$$\Rightarrow T(n) = 8 \cdot T(\tfrac{n}{2}) + n^2$$

Master Theorem

Master Theorem: $T(n) = a \cdot T(\frac{n}{b}) + f(n)$

Falls gilt:	Dann folgt:
$f(n) \in \mathcal{O}(n^{\log_b(a-\varepsilon)})$	$T(n) \in \Theta(n^{\log_b(a)})$
$f(n) \in \Theta(n^{\log_b(a)})$	$T(n) \in \Theta(n^{log_b(a)} \cdot \log(n))$
$f(n) \in \Omega(n^{\log_b(a+\varepsilon)})$	$T(n) \in \Theta(f(n))$

- $T(n) = 8 \cdot T(n/2) + n^2$

(1) $\log_b(a) = \log_2(8) = 3$

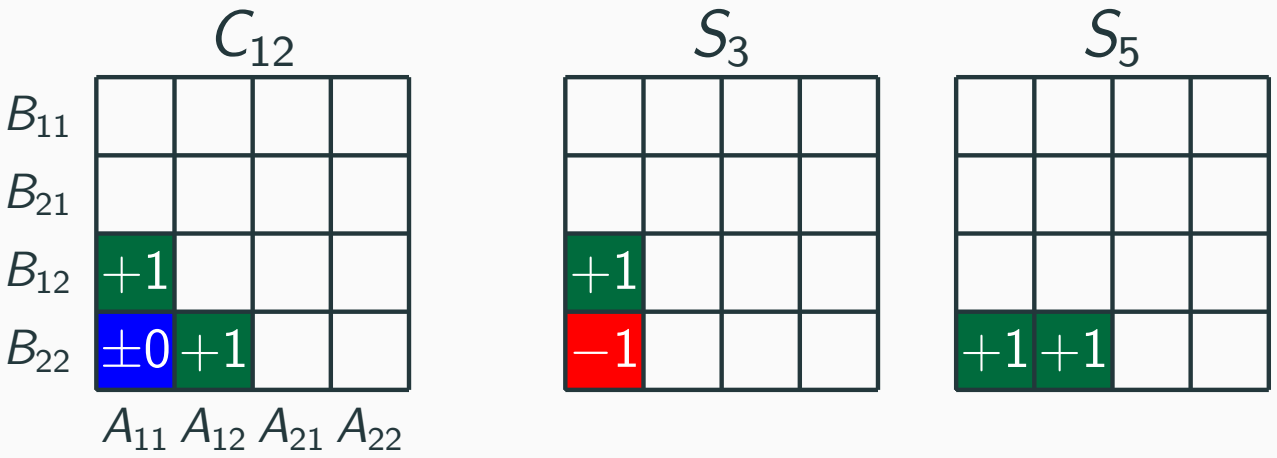
(2) $f(n) = n^2 \in \mathcal{O}(n^{\log_2(8-\varepsilon)})$

(3) $T(n) \in \Theta(n^{log_b(a)}) = \Theta(n^3)$

$\Big\} \; S(MM) = \mathcal{O}(n^3)$

$\Rightarrow$ Solange $2 \leq log_b(a) < 3$ gilt $T(n) \in \Theta(n^{\log_b(a)})$

Strassen Algorithmus



$$C_{12} = S_3 + S_5 = A_{11} \cdot (B_{12} - B_{22}) + (A_{11} + A_{12}) \cdot B_{22}$$

$$= A_{11}B_{12} - A_{11}B_{22} + A_{11}B_{22} + A_{12}B_{22} = A_{11}B_{12} + A_{12}B_{22}$$

$$C_{11} = S_1 + S_4 - S_5 + S_7 \qquad C_{12} = S_3 + S_5$$

$$C_{21} = S_2 + S_4 \qquad C_{22} = S_1 - S_2 + S_3 + S_6$$

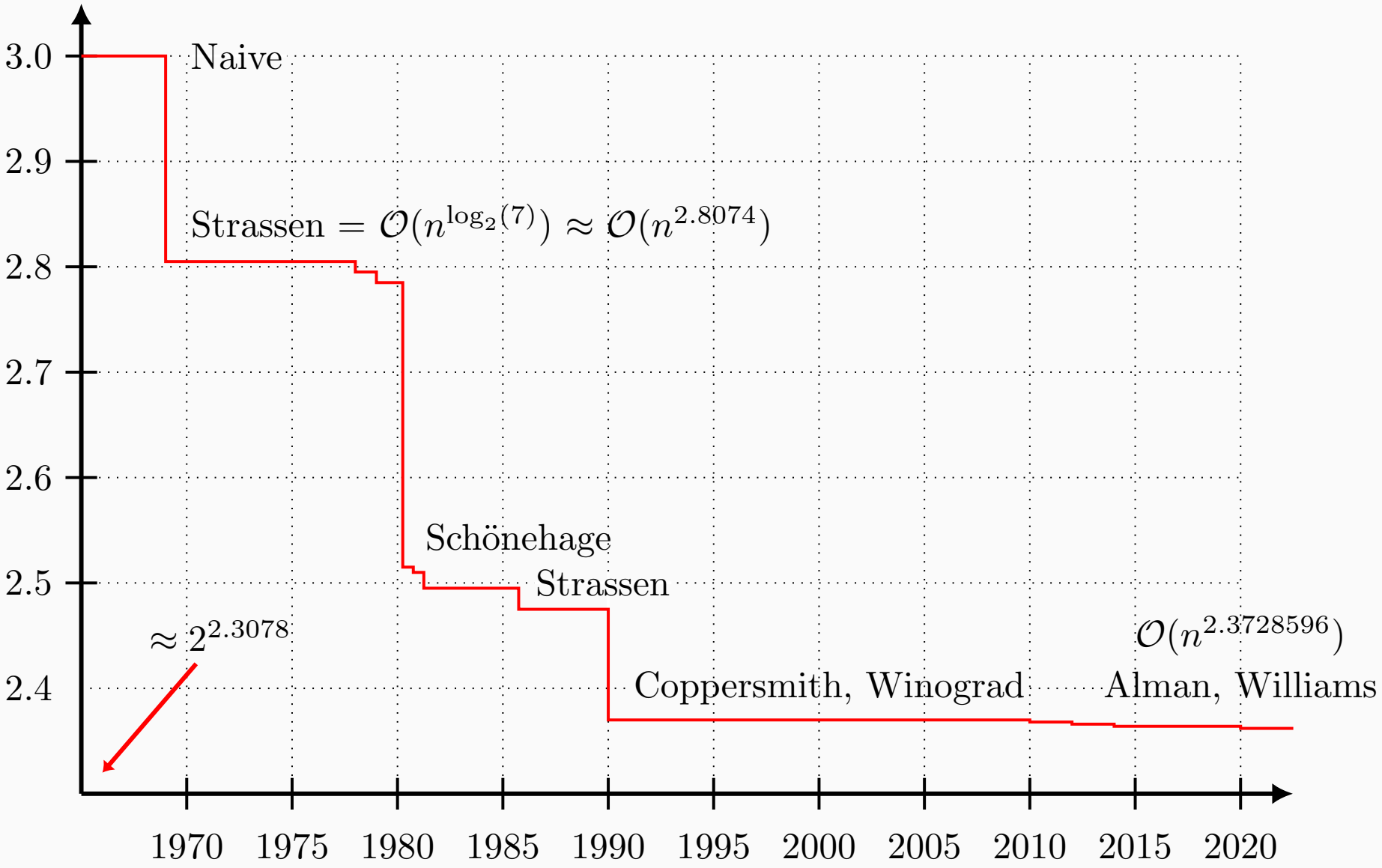
$$S_1 = (A_{11} + A_{22}) \cdot (A_{22} + B_{22}) \qquad S_5 = (A_{11} + A_{12}) \cdot B_{22}$$

$$S_2 = (A_{21} + A_{22}) \cdot B_{11} \qquad S_6 = (A_{21} - A_{11}) \cdot (B_{11} + B_{12})$$

$$S_3 = A_{11} \cdot (B_{12} - B_{22}) \qquad S_7 = (A_{12} - A_{22}) \cdot (B_{21} + B_{22})$$

$$S_4 = A_{22} \cdot (B_{21} - B_{11})$$

Matrix Multiplikation: Timeline



Determinante

- $\mathrm{DET}(A) = \sum_{\sigma \in S_n} \left(\mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma_i} \right)$, $A \in \mathbb{K}^{n \times n}$, $n \in \mathbb{N}$

$$A = \left(\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array} \right)$$

$$\begin{aligned} \det(A) = {} & + a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ & - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} \end{aligned}$$

- Es gibt $n!$ Summanden $\leftrightarrow$ Anzahl der Permutationen

Komplexität

Laplace Expansion	$\mathcal{O}(n!)$
LU Dekomposition	$\mathcal{O}(n^3)$
$\mathcal{O}(\mathrm{S}(MM)log(n))$	$\mathcal{O}(n^{2.37286...})$

- **Achtung:** Gauss Elimination nutzt *Division*

$\rightarrow$ Hier nicht erlaubt!

- Determinante als Produkt von Matrizen

$$\begin{aligned} \mathrm{L}(DET) &= \mathcal{O}(n^{\log(n)}) \\ \hline \mathrm{L}(DET) &= \Omega(n^3) \end{aligned}$$

Permanente

- $\mathrm{PER}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma_i}$, $A \in \mathbb{K}^{n \times n}$, $n \in \mathbb{N}$

- Große Schwester der Determinante
- Es gibt $n!$ Summanden!

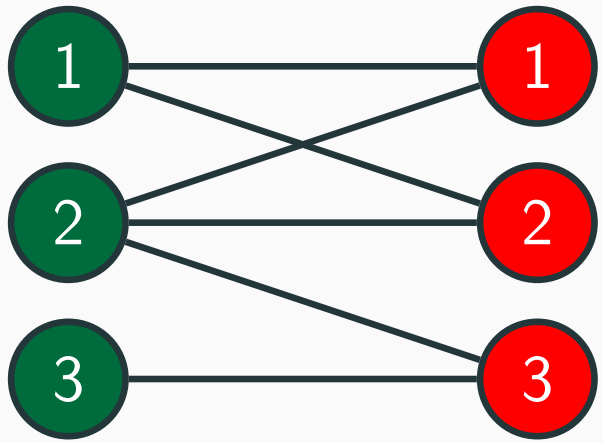
- Bezug in der Graphentheorie:

$\rightarrow$ Zählt perfekte Matchings in Bipartiten Graphen

$\rightarrow$ Jedes Monom $\neq 0$ entspricht einem Matching

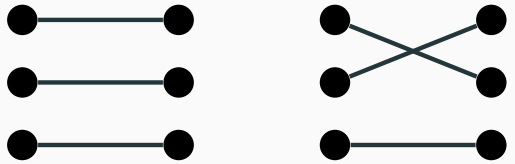
Beispiel: Bipartites Matching

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array} \begin{array}{c} \begin{array}{ccc} b_1 & b_2 & b_3 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$



$$m_{11} \cdot m_{22} \cdot m_{33} = 1$$

$$m_{12} \cdot m_{21} \cdot m_{33} = 1$$



$\Rightarrow PER(M) = 2$

$\Rightarrow$ Es gibt 2 Matchings

Ryser Formel

- $\mathrm{PER}(A) = (-1)^n \sum_{S \subseteq \{1,\ldots,n\}} (-1)^{|S|} \prod_{i=1}^{n} \sum_{j \in S} a_{ij}$

$$\left.\begin{array}{ll} S = \{1,2\} & (a_{11} + a_{12})(a_{21} + a_{22}) \\ S = \{1\} & -a_{11}a_{21} \\ S = \{2\} & -a_{12}a_{22} \end{array}\right\} a_{11}a_{22} + a_{12}a_{21}$$

	Ryser	**Ryser + Gray code**
Additionen:	$n(n-2)2^{n-1}$	$(n-1)(2^n-1)$
Multiplik.:	$n(2^n-2)$	$(n-1)(2^n-1)$

Komplexität

- Ryser-Formel entspricht $\sum \prod \sum$-Formel
- Gray-Code gibt keine kleinere Formel, nur Schaltkreis

Theorem

$L(PER) = \mathcal{O}(n^2 2^n)$

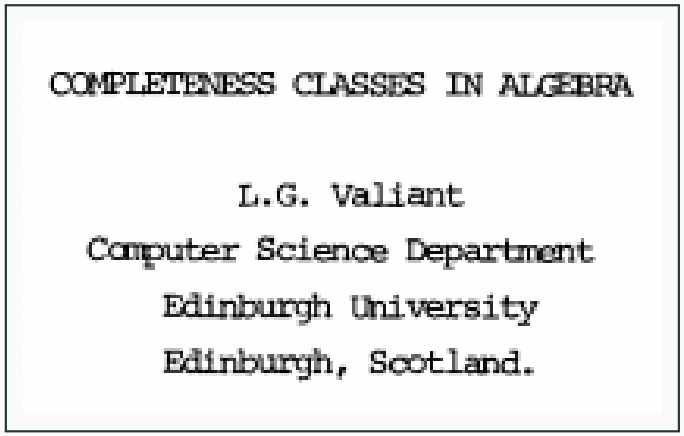
- **Annahme:** $S(PER) \neq n^{\mathcal{O}(1)}$
- Bedeutung in mehreren Komplexitätsklassen

$\rightarrow$ $\{0,1\}$-Permanente ist $\#\mathcal{P}$-vollständig

Erinnerung: Klasse von Zählproblemen

$\rightarrow$ #SAT, Anzahl Matchings in einem bipartiten Graphen

Valiant's Komplexitätsklassen



COMPLETENESS CLASSES IN ALGEBRA

L.G. Valiant
Computer Science Department
Edinburgh University
Edinburgh, Scotland.

Eingeführt von *Leslie Valiant* in 1979

- (Teilweise) Analoge Klassen zu $\mathcal{P}$ und $\mathcal{NP}$

$\rightarrow$ $\mathcal{VP}$ und $\mathcal{VNP}$ (Valiant $\mathcal{P}$ & $\mathcal{NP}$)

- **Projektion** als Reduzierbarkeit bei Polynomen
- Einstufung der besprochenen Beispiele

Die Klasse $\mathcal{VP}$

Definition

Eine Sequenz von Polynomen $f = \{f_n\}$ ist in $\mathcal{VP}$ wenn $S(f) \leq n^{\mathcal{O}(1)}$.

- Alle Polynome die von arithmetischen Schaltkreisen polynomieller Größe berechnet werden können

$\Rightarrow$ SYM, MM, DET sind alle in $\mathcal{VP}$

- Unterklasse $\mathcal{VL}$ aller Polynome mit polynomiellen Formeln

$\rightarrow$ DET ist $\mathcal{VP}$-hard

$\Leftrightarrow$ $\forall f = \{f_n\} \in \mathcal{VL}, \forall n\colon\ f_n \leq DET_{n^{\mathcal{O}(1)}}$

Affine Projektion

Definition

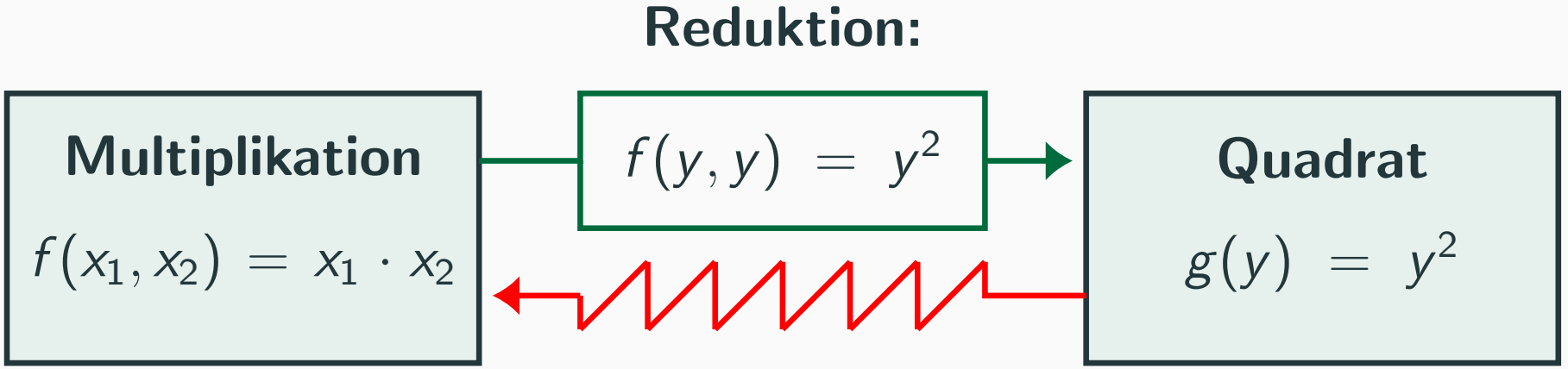
Seien $f \in \mathbb{F}[x_1, \cdots, x_n]$ und $g \in \mathbb{F}[y_1, \cdots, y_m]$, dann ist f eine **affine Projektion** $f \leq g$ von g, wenn m affine Funktionen $l_i : \mathbb{F}^n \to \mathbb{F}$ existieren, so dass $f(x) = g(l_1(x), \cdots, l_m(x))$. f ist eine **Projektion** von g, wenn alle affinen Funktionen l_i von maximal einer Variablen abhängig sind.

$\Rightarrow$ Falls $f \leq g$ folgt $\mathrm{S}(f) \leq \mathrm{S}(g) + \mathcal{O}(mn)$

- Relation ist Transitiv

$\rightarrow$ Partielle Ordnung der Komplexität von Polynomen

Affine Projektion: Idee



- Variablen können skaliert oder ganz ausgetauscht werden

$\rightarrow$ $y_i = a \cdot x_j + b$ für ein beliebiges $j \in \{1, \ldots, n\}$

- Variablen können weggelassen werden mit $y_i = 0$

Die Klasse $\mathcal{VNP}$

Definition

Eine Sequenz von Polynomen $f = \{f_n\} \in \mathbb{F}[x_1, \cdots, x_n]$ ist in $\mathcal{VNP}$ wenn es ein $g = \{g_n\} \in \mathbb{F}[x_1, \cdots, x_n, y_1, \cdots, y_n] \in \mathcal{VP}$ gibt, so dass $f_n(x) = \sum_{\alpha \in \{0,1\}^n} g_n(x, \alpha)$.

- Wähle $f = g$, $f \in \mathcal{VP} \Rightarrow \mathcal{VP} \subseteq \mathcal{VNP}$
- Koeffizienten von Monomen in f in polynomieller Zeit
- *PER* ist $\mathcal{VNP}$-vollständig

Zusammenhänge

Bezug:

- Direkter Bezug zur Klasse $\#\mathcal{P}$
- Eher indirekter Bezug zun den Klassen $\mathcal{P}$ und $\mathcal{NP}$

Fakten:

- $\mathcal{P} \neq \mathcal{NP} \Rightarrow \mathcal{VP} \neq \mathcal{VNP}$
- $\mathcal{VP} \neq \mathcal{VNP} \Rightarrow \mathcal{P}/poly \neq \mathcal{NP}/poly$

Vermutung:

- $\mathcal{VP} \neq \mathcal{VNP}$

Monotone Schaltkreise

- *Junge* Wissenschaft, bisher wenig Schranken

$\Rightarrow$ Eingeschränkte Modelle für stärkere Schranken

Monotone Schaltkreise

- Nur positive Koeffizienten des Körpers
- Vergleichbar mit boolschen Schaltkreisen ohne Negation

Theorem

Es existiert ein positives Polynom $f \in \mathcal{VP}$, das monotone Schaltkreise der Größe $\exp(n)$ benötigt.

Nicht-kommutative Schaltkreise

- Variablen in einem Monom nicht vertauschbar
- $x^2 - y^2$ bisher eine Multiplikation $(x - y) \cdot (x + y)$

$\Rightarrow$ Jetzt $x^2 - y^2 + xy - yx \rightarrow$ Nicht mehr möglich!

- $DET \leq PER$ und $PER \leq DET$

Theorem

PER und DET benötigen nicht-kommutative Formeln der Größe $exp(n)$.

Vielen Dank!