Complexiteit

College 6

Docent: Lieuwe Vinkhuijzen

2 maart 2020

Nieuws

Huiswerkogpave 1:
liacs.leidenuniv.nl/~vinkhuijzenlt/complexiteit
Deadline: Vandaag 23:59

Huiswerkopgave 2: Volgende week online
Deadline: 30 maart 23:59

Vorige week

- Perfect matching oplossen met SAT
- Beslissingsboom argument voor sorteren in $\Omega(n \log(n))$
- Selectie/mediaan zoeken in array
- Polynoom evalueren
- Getallen vermenigvuldigen

Deze week

1. Circuit Gelijkheid oplossen met circuit SAT
2. Circuit SAT oplossen met CNF-SAT
3. Getallen vermenigvuldigen in $\mathcal{O}(n^{\log_2(3)}) \approx \mathcal{O}(n^{1.58})$
4. Matrix vermenigvuldigen in $\mathcal{O}(n^{\log_2(7)}) \approx \mathcal{O}(n^{2.81})$

Boolse circuits

Bools circuit: Inputs $x_1, x_2, \ldots, x_n$, elke gate is $\wedge$ (AND), of $\vee$ (OR), of $\neg$ (NOT), er is één "output" gate.
Een circuit C berekent een functie $C\colon \{0,1\}^n \to \{0,1\}$.

(Voorbeelden op het bord)

Circuit gelijkheid

Input: Twee Boolse circuits C, D met inputs $x_1, \ldots, x_n$, met $\wedge$ (AND), $\vee$ (OR) en $\neg$ (NOT) gates, allebei één output gate.
Output: "Ja", als de circuits dezelfde functie berekenen, dus als voor alle toekenningen aan de variabelen $x_1, \ldots, x_n$, geldt dat $C(x) = D(x)$.

Circuit Satisfiability

Input: Een Bools circuit C met inputs $x_1, \ldots, x_n$ en één output gate, en met $\wedge$ (AND), $\vee$ (OR) en $\neg$ (NOT) gates.
Output: "Ja" d.e.s.d.a. er een toekenning aan $x_1, \ldots, x_n$ bestaat die het circuit $\textsc{True}$ doet outputten.

Circuit gelijkheid oplossen met Circuit Satisfiability

Input: Twee Boolse n-inputs $\{\wedge, \vee, \neg\}$ circuits C, D.
Output: "Ja" d.e.s.d.a. voor alle toekenningen aan de variabelen $x_1, \ldots, x_n$, geldt dat $C(\vec{x}) = D(\vec{x})$.

Circuit gelijkheid oplossen met Circuit Satisfiability

Input: Twee Boolse n-inputs $\{\wedge, \vee, \neg\}$ circuits C, D.
Output: "Ja" d.e.s.d.a. voor alle toekenningen aan de variabelen $x_1, \ldots, x_n$, geldt dat $C(\vec{x}) = D(\vec{x})$.

Lemma

Het circuit E is satisfiable d.e.s.d.a. $C \neq D$.

Bewijs.

($\implies$) Stel dat $\vec{x}$ een satisfying assignment is van E. Dan is $C(\vec{x}) \neq D(\vec{x})$. □

Circuit gelijkheid oplossen met Circuit Satisfiability

Input: Twee Boolse n-inputs $\{\wedge, \vee, \neg\}$ circuits C, D.
Output: "Ja" d.e.s.d.a. voor alle toekenningen aan de variabelen $x_1, \ldots, x_n$, geldt dat $C(\vec{x}) = D(\vec{x})$.

Lemma

Het circuit E is satisfiable d.e.s.d.a. $C \neq D$.

Bewijs.

$(\Longleftarrow)$ Stel dat $C \neq D$. Dan is er $\vec{x}$ met $C(\vec{x}) \neq D(\vec{x})$. Dus $E(\vec{x}) = \textsc{True}$. $\square$

Circuit Satisfiability oplossen met CNF Satisfiability

Input: Een Bools $\{\wedge, \vee, \neg\}$-circuit C met inputs $x_1, \ldots, x_n$ en één output.
Output: "Ja" d.e.s.d.a. er een toekenning aan $x_1, \ldots, x_n$ bestaat die het circuit $\textsc{True}$ doet outputten.

Circuit Satisfiability oplossen met CNF Satisfiability

Input: Een Bools $\{\wedge, \vee, \neg\}$-circuit C met inputs $x_1, \ldots, x_n$ en één output.
Output: "Ja" d.e.s.d.a. er een toekenning aan $x_1, \ldots, x_n$ bestaat die het circuit $\textsc{True}$ doet outputten.

Observatie: elke CNF formule is een circuit van 3 lagen "diep".
Observatie: We kunnen ervoor zorgen dat alle gates een in-degree hebben van 1 of 2.
Voorbeeld CNF: $\phi = (x_1 \vee x_2) \wedge (\neg x_1 \vee x_3) \wedge (\neg x_1 \vee x_4)$

Circuit Satisfiability oplossen met CNF Satisfiability

Input: Een Bools $\{\wedge, \vee, \neg\}$-circuit C met inputs $x_1, \ldots, x_n$ en één output.
Output: "Ja" d.e.s.d.a. er een toekenning aan $x_1, \ldots, x_n$ bestaat die het circuit TRUE doet outputten.

Plan. We maken een CNF formule ϕ die *satisfiable* is d.e.s.d.a. C satisfiable is.
We "encoderen" de goede toekenningen aan C, in ϕ.
Zeg dat C, k gates heeft, $g_1, \ldots, g_k$. De formule ϕ heeft dan $n + k$ variabelen, namelijk $x_1, \ldots, x_n, g_1, \ldots, g_k$.

Circuit Satisfiability oplossen met CNF Satisfiability

Input: Een Bools $\{\wedge, \vee, \neg\}$-circuit C met inputs $x_1, \ldots, x_n$ en één output.
Output: "Ja" d.e.s.d.a. er een toekenning aan $x_1, \ldots, x_n$ bestaat die het circuit $\textsc{True}$ doet outputten.

$$\phi = (g_6) \wedge (g_6 = (g_4 \vee g_5)) \wedge (g_5 = (g_1 \wedge g_3)) \wedge (g_4 = (x_1 \wedge g_2)) \\ \wedge (g_2 = (x_2 \vee x_3)) \wedge (g_3 = (x_3 \wedge x_3)) \wedge (g_1 = \neg x_1)$$

Staat nog niet in CNF, maar gaat de goede kant op.

Lemma

C is satisfiable d.e.s.d.a. ϕ satisfiable is.

Circuit Satisfiability oplossen met CNF Satisfiability

Input: Een Bools $\{\wedge, \vee, \neg\}$-circuit C met inputs $x_1, \ldots, x_n$ en één output.
Output: "Ja" d.e.s.d.a. er een toekenning aan $x_1, \ldots, x_n$ bestaat die het circuit $\textsc{True}$ doet outputten.

$$\begin{aligned}\phi = (g_6) \wedge (g_6 = (g_4 \vee g_5)) \wedge (g_5 = (g_1 \wedge g_3)) \wedge (g_4 = (x_1 \wedge g_2)) \\ \wedge (g_2 = (x_2 \vee x_3)) \wedge (g_3 = (x_3 \wedge x_3)) \wedge (g_1 = \neg x_1)\end{aligned}$$

Staat nog niet in CNF, maar gaat de goede kant op.

Lemma

C is satisfiable d.e.s.d.a. ϕ satisfiable is.

Naar CNF met DeMorgan's wetten (op het bord)

Getallen vermenigvuldigen in $O(n^{\log_2(3)})$

Input: Twee getallen, $a = a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + \cdots a_n 10^n$, $b = b_0 + b_1 10 + b_2 10^2 + \cdots b_n 10^n$.
Output: Het product $c = a \times b$.

Anatoly Karatsuba's algoritme
Tijd: $T(n) \in O(n^{\log_2(3)}) \approx O(n^{1.58})$

Input: Twee getallen,
$a = a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + \cdots a_n 10^n$,
$b = b_0 + b_1 10 + b_2 10^2 + b_3 10^3 + \cdots b_n 10^n$.
Output: Het product $c = a \times b$.

---

procedure $\textsc{Karatsuba}(a, b)$
    if $n = 0$ **then**
        return $a_0 \times b_0$
    end if
    $laag_1 := a \mod 10^{\frac{n+1}{2}}$ ▷ Least significant digits
    $laag_2 := b \mod 10^{\frac{n+1}{2}}$
    $hoog_1 := a >> \frac{n+1}{2}$
    $hoog_2 := b >> \frac{n+1}{2}$
    $m_1 := Karatsuba(laag_1, laag_2)$
    $m_2 := Karatsuba(hoog_1, hoog_2)$
    $m_3 := Karatsuba(laag_1 + hoog_1, laag_2 + hoog_2)$
    $m_4 := m_3 - m_1 - m_2$
    return $m_1 + m_3 \times 10^{\frac{n+1}{2}} + m_2 \times 10^n$
end procedure

Karatsuba's algoritme

$$T(n) = \begin{cases} 1 & \text{Als } n = 1 \\ 3T(\frac{1}{2}n) + 4n & \text{Als } n > 1 \end{cases}$$

$$T(n) = 4n + 3T(\tfrac{1}{2}n) = 4n + 6n + 3^2T(\tfrac{1}{4}n) =$$

Matrix vermenigvuldiging in $O(n^{\log_2(7)})$

Input: Twee $n \times n$ matrices van gehele getallen A, B
Output: Het product $C = A \cdot B$

Matrix vermenigvuldiging in $O(n^3)$

Input: Twee $n \times n$ matrices van gehele getallen A, B
Output: Het product $C = A \cdot B$

$$A = \begin{bmatrix} A_{1,1} & A_{1,2} \\ A_{21} & A_{2,2} \end{bmatrix} B = \begin{bmatrix} B_{1,1} & B_{1,2} \\ B_{21} & B_{2,2} \end{bmatrix}$$

$$C = A \cdot B = \begin{bmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{bmatrix}$$

Matrix vermenigvuldiging in $O(n^3)$

Input: Twee $n \times n$ matrices van gehele getallen A, B
Output: Het product $C = A \cdot B$

```
procedure MatMul(A, B)
    for i = 1 ... n do
        for j = 1 ... n do
            C_{i,j} := 0
            for k = 1 ... n do
                C_{i,j} := C_{i,j} + A_{i,k} × B_{k,j}
            end for
        end for
    end for
    return C
end procedure
```

Matrix vermenigvuldiging in $O(n^3)$

Input: Twee $n \times n$ matrices van gehele getallen A, B
Output: Het product $C = A \cdot B$

Plan: Verdeel en heers. Neem het geval dat A een $2^k \times 2^k$ matrices zijn.

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} B = \begin{bmatrix} B_{1,1} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

$$C = A \cdot B = \begin{bmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{bmatrix}$$

Aantal optellingen: 4
Aantal vermenivuldigingen: 8

Matrix vermenigvuldiging in $O(n^3)$

Input: Twee $n \times n$ matrices van gehele getallen A, B
Output: Het product $C = A \cdot B$

Aantal optellingen:

$$A(n) = \begin{cases} 0 & \text{Als } n = 1 \\ 8A(\frac{1}{2}n) + n^2 & \text{Als } n > 1 \end{cases} \quad = \quad \frac{4}{3}n^2 \tag{1}$$

Aantal vermenigvuldigingen:

$$M(n) = \begin{cases} 8 & \text{Als } n = 2 \\ 8M(\frac{1}{2}n) & \text{Als } n > 2 \end{cases} \quad = \quad 8^{\log_2(n)} = 3^n \tag{2}$$

Matrix vermenigvuldiging in $O(n^3)$

Input: Twee $n \times n$ matrices van gehele getallen A, B
Output: Het product $C = A \cdot B$

Aantal optellingen:

$$A(n) = \begin{cases} 0 & \text{Als } n = 1 \\ 8A(\frac{1}{2}n) + n^2 & \text{Als } n > 1 \end{cases} \quad = \quad \frac{4}{3}n^2 \tag{3}$$

Aantal vermenigvuldigingen:

$$M(n) = \begin{cases} 8 & \text{Als } n = 2 \\ 8M(\frac{1}{2}n) & \text{Als } n > 2 \end{cases} \quad = \quad 8^{\log_2(n)} = n^3 \tag{4}$$