Algebraic method in the theory of synthesis

I.S. Sergeev, 2021

Problem: compute (fast) an operator $S : A \to A$

Solution: transition from a structure A to a structure B

$$S = T' \circ S' \circ T$$

$$\begin{tikzcd} A \arrow[r, "T"] \arrow[d, "S"'] & B \arrow[d, "S'"] \\ A & B \arrow[l, "T'"] \end{tikzcd}$$

Type I: $A \cong B$ (change of representation; appropriate encoding)

Type II: purely algebraic method

Standard representation $\mathbb{C} \cong \mathbb{R}^2$: $x + \mathbf{i}y \to [x,\ y]$:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} \in \mathbb{C}; \qquad \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \pm \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \pm x_2 \\ y_1 \pm y_2 \end{bmatrix}, \qquad \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \cdot \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1x_2 - y_1y_2 \\ x_1y_2 + y_1x_2 \end{bmatrix}.$$

Multiplication via the Karatsuba method:

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \cdot \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1x_2 - y_1y_2 \\ (x_1 + y_1)(x_2 + y_2) - x_1x_2 - y_1y_2 \end{bmatrix}.$$

Complexity: $\quad A_{\mathbb{C}} = 2A_{\mathbb{R}}, \qquad M_{\mathbb{C}} = 4M_{\mathbb{R}} + 2A_{\mathbb{R}}$ or $\underline{M_{\mathbb{C}} = 3M_{\mathbb{R}} + 5A_{\mathbb{R}}}$.

Extended representation $\mathbb{C} \to \mathbb{R}^3$: $x + \mathbf{i}y \to [x,\ y,\ x + y]$:

$$\begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} \in \mathbb{C}; \qquad \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} \pm \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = \begin{bmatrix} x_1 \pm x_2 \\ y_1 \pm y_2 \\ z_1 \pm z_2 \end{bmatrix}, \qquad \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} \cdot \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = \begin{bmatrix} x_1x_2 - y_1y_2 \\ z_1z_2 - x_1x_2 - y_1y_2 \\ z_1z_2 - 2y_1y_2 \end{bmatrix}.$$

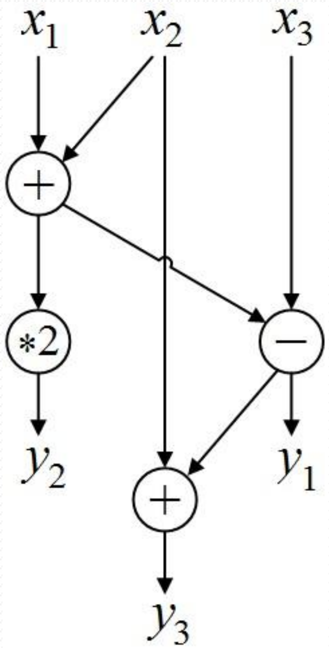
Complexity: $\quad A_{\mathbb{C}} = 3A_{\mathbb{R}}, \qquad M_{\mathbb{C}} = 3M_{\mathbb{R}} + 4A_{\mathbb{R}}$ or $\underline{M_{\mathbb{C}} = 3M_{\mathbb{R}} + 3A_{\mathbb{R}} + D_{\mathbb{R}}}$.

Transition: $\quad \mathbb{R}^2 \to \mathbb{R}^3: \quad A_{\mathbb{R}}; \qquad \mathbb{R}^3 \to \mathbb{R}^2: \quad 0.$

Complexity of *abcd* : $\quad \mathbb{R}^2: \quad 9M_{\mathbb{R}} + 15A_{\mathbb{R}}, \qquad \mathbb{R}^3: \quad 9M_{\mathbb{R}} + 13A_{\mathbb{R}} + 3D_{\mathbb{R}}.$

Complexity and depth of circuits

circuit S:



$$y = A \cdot x$$

$$A = \begin{bmatrix} 1 & 1 & -1 \\ 2 & 2 & 0 \\ 1 & 2 & -1 \end{bmatrix}$$

basis: $B = \{x + y, x - y, 2x\}$

complexity = number of elements: $\mathsf{C}_B(S) = 4$

depth = length of the longest input-output path: $\mathsf{D}_B(S) = 3$

complexity (depth) of a function F = minimal complexity (depth) of a circuit computing it: $\mathsf{C}_B(F),\ \mathsf{D}_B(F)$

Boolean matrix multiplication

$R = (\{0,1\}, \vee, \wedge) : \qquad Z = XY \qquad X, Y, Z \in R^{n\times n}$

$\mathsf{C}_{\{\vee,\wedge\}}(Z) = 2n^3 - n^2$ (M. Paterson'75)

$R \to \mathbb{Z}_{n+1} : \qquad 0 \to 0, \quad 1 \to 1$

$\mathbb{Z}_{n+1} \to R : \qquad 0 \to 0, \quad 1, \ldots, n \to 1$

$Z' = X'Y' : \quad \text{complexity } \mathsf{C}_{\{\pm,*\}}(Z') = n^{\omega+o(1)}, \;\; \omega < 2.38$

T. $\mathsf{C}_{B_2}(Z) \preceq \log^2 n \cdot \mathsf{C}_{\{\pm,*\}}(Z')$ (1970s)

Integer multiplication → polynomial multiplication

A,*B* – *n*-bit numbers

$$\mathbb{Z} \to \mathbb{Z}[x]: \qquad [A_1 A_0] \to A_1 x + A_0, \quad x = 2^{n/2}$$

(A.A. Karatsuba'62)

$$[A_{r-1} A_{r-2} \ldots A_0] \to A_{r-1} x^{r-1} + \ldots + A_1 x + \ldots + A_0, \quad x = 2^{n/r}$$

(A.L. Toom'63)

Interpolation:

Karatsuba method: $\mathbb{Z}[x] \to \mathbb{Z}^3: \quad F(x) \to (\, F(0), F(1), F(\infty)\,)$

$$\mathsf{C}(A \cdot B) \preceq n^{\log_2 3}$$

Toom's method: $\mathbb{Z}[x] \to \mathbb{Z}^{2r-1}: \quad F(x) \to (\, F(0), F(\pm 1), \ldots, F(\pm(r-1))\,)$

$$r = 2^{\Theta(\sqrt{\log n})} \quad \to \quad \mathsf{C}(A \cdot B) \preceq n \cdot 2^{O(\sqrt{\log n})}$$

Integer multiplication $\rightarrow$ DFT

$$\mathbb{Z} \to \mathbb{C}[x]/(x^k - 1) \to \mathbb{C}^k : \quad F(x) \xrightarrow{\text{DFT}} (\, F(\zeta^0), F(\zeta^1), \ldots, F(\zeta^{k-1})\,)$$

$$\mathsf{C}(A \cdot B) \preceq n \log n \cdot \log\log n \cdot \log\log\log n \ldots$$

(A.A. Karatsuba'67; A. Schönhage, V. Straßen'71)

$$\mathbb{Z} \to \mathbb{Z}_{\Phi_m}[x]/(x^{2^{m+1}} - 1), \quad \Phi_m = 2^{2^m} + 1$$

$\mathsf{C}(A \cdot B) \preceq n \log n \cdot \log\log n$ (A. Schönhage, V. Straßen'71)

$$\mathbb{Z} \to C_p[y]/(y^{2^{ps}} - 1), \quad C_p = \mathbb{C}[x]/(x^{2^p} + 1)$$

$\mathsf{C}(A \cdot B) \preceq n \log n \cdot 2^{O(\log^* n)}$ (M. Fürer'07)

$$\mathbb{Z} \to C_p[x_1, \ldots, x_d]/(x_1^{n_1} - 1, \ldots, x_d^{n_d} - 1)$$

$\mathsf{C}(A \cdot B) \preceq n \log n$ (D. Harvey, J. van der Hoeven'19)

DFT over field of complex numbers

linear basis: $\Lambda^F = \{x \pm y\} \cup \{ax \mid a \in F\}$

Cooley—Tukey scheme: $\mathrm{DFT}_{PQ} = [\bigotimes \mathrm{DFT}_P] \circ [\bigotimes \zeta^{ij}] \circ [\bigotimes \mathrm{DFT}_Q]$

$N = 2^k$: $\mathsf{C}_{\Lambda^{\mathbb{C}}}(\mathrm{DFT}_N) \le 1.5N \log_2 N$ (J. Cooley, J. Tukey'65)

$\Longrightarrow$ $\mathsf{C}_{\Lambda^{\mathbb{R}}}(\mathrm{DFT}_N) \le 5N \log_2 N$ $(A_{\mathbb{C}} = 2A_{\mathbb{R}},\quad S_{\mathbb{C}} = 3S_{\mathbb{R}} + 3A_{\mathbb{R}})$

split-radix FFT: $\mathsf{C}_{\Lambda^{\mathbb{R}}}(\mathrm{DFT}_N) \le 4N \log_2 N$

(P. Duhamel, H. Hollmann, J.-B. Martens, M. Vetterli, H. Nussbaumer'84)

$(x_1, \ldots, x_N) \to (\sigma_1 x_1, \ldots, \sigma_N x_N)$

$\mathsf{C}_{\Lambda^{\mathbb{R}}}(\mathrm{DFT}_N) \le 3\frac{7}{9} N \log_2 N$ (J. van Buskirk'04)

$S_{\mathbb{C}}[\pm 1 + a\mathbf{i};\ a \pm \mathbf{i}] = 2S_{\mathbb{R}} + 2A_{\mathbb{R}}$

$$\sigma_j = \prod_{l \ge 0} \max\left\{ \left|\cos \frac{4^l 2\pi j}{N}\right|, \left|\sin \frac{4^l 2\pi j}{N}\right| \right\}$$

$\mathsf{C}_{\Lambda^{\mathbb{R}}}(\mathrm{DFT}_N) \lesssim 3.76875 N \log_2 N$ $\sigma_j^{16} = 1$ (I.S. Sergeev'17)

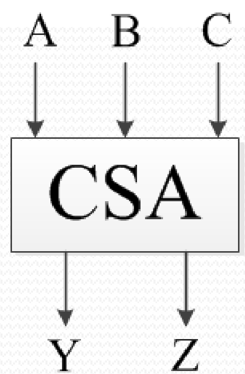
Integer multiplication depth

$$\times\ \begin{matrix} a_3a_2a_1a_0 \\ b_3\,b_2\,b_1\,b_0 \end{matrix} \quad \rightarrow \quad + \begin{array}{ccccccc} & & & a_0b_3 & a_0b_2 & a_0b_1 & a_0b_0 \\ & & a_1b_3 & a_1b_2 & a_1b_1 & a_1b_0 & \\ & a_2b_3 & a_2b_2 & a_2b_1 & a_2b_0 & & \\ a_3b_3 & a_3b_2 & a_3b_1 & a_3b_0 & & & \end{array} \quad \rightarrow \quad + \begin{matrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{matrix}$$

<u>Parallel addition of *n* bits</u>

method of compressors (1960s):

compressor (CSA): *A*+*B*+*C*=*X*+*Y*, depth *O*(1)



$$\mathsf{D}_{B_2}(A \cdot B) \lesssim \mathsf{D}_{B_2}(x_1 + \ldots + x_n) + \log_2 n$$

$\mathsf{D}_{B_2}(x_1 + \ldots + x_n) \lesssim 3.71 \log_2 n$ (M. Paterson, N. Pippenger, U. Zwick'92)

encoding: $x \rightarrow (x^\vee, y^\vee, x^\wedge, y^\wedge), \quad x = x^\vee \vee y^\vee, \quad x = x^\wedge \cdot y^\wedge$

$\mathsf{D}_{B_2}(x_1 + \ldots + x_n) \lesssim 3.44 \log_2 n$ (M. Paterson, U. Zwick; E. Grove'93)

$\mathbb{Z} \rightarrow \mathbb{Z}_{2^k} \times \mathbb{Z}_{3^l}, \quad 2^k \cdot 3^l > n$

$\mathsf{D} \lesssim 3.34 \log_2 n \qquad \ldots \qquad 3.02 \log_2 n$ (I.S. Sergeev'13-16)

Depth of addition modulo 7

$\mathbb{Z}_7 :$ binary representation (b_2, b_1, b_0);

alternative representation $(s_0, s_1, \ldots, s_6)$ $\quad s_k(x) = \begin{cases} 1, & x = k \\ 0, & x \neq k \end{cases}$

$$s_k(x+y) = \bigvee_{r=0}^{6} s_r(x) \cdot s_{k-r \bmod 7}(y)$$

$$\Rightarrow \quad \mathsf{D}_{B_2}(x_1 + \ldots + x_n \bmod 7) \leq 4\log_2 n$$

$$(\mathsf{D}_{B_2}(x_1 + \ldots + x_n \bmod 7) \lesssim \mathsf{D}_{B_2}(x_1 + \ldots + x_n) \lesssim 3.02\log_2 n)$$

$\mathbb{Z}_7 \to GL(3, \mathbb{Z}_2) \subset \mathbb{Z}_2^{3\times 3}$ (D. van Leijenhorst'87)

matrix representation:

$$\begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & h_{33} \end{bmatrix}$$

$$h_{ik}(x+y) = \bigoplus_{j=1}^{3} h_{ij}(x) \cdot h_{jk}(y)$$

$$\Rightarrow \quad \mathsf{D}_{B_2}(x_1 + \ldots + x_n \bmod 7) \leq 3\log_2 n + O(1)$$

$\ldots \quad \mathsf{D} \leq 2.93\log_2 n + O(1)$ (I.S. Sergeev'16)

Open research directions

Matrix multiplication: group-theoretic approach

(H. Cohn, C. Umans'03 ...)

$$\mathbb{C}^{n\times n} \to \mathbb{C}[G]: \qquad \|a_{ij}\| \to \sum_{i,j} a_{ij}\cdot s_i t_j^{-1}, \quad \|b_{ij}\| \to \sum_{i,j} b_{ij}\cdot t_i u_j^{-1}, \quad \|c_{ij}\| \to \sum_{i,j} c_{ij}\cdot s_i u_j^{-1}$$

$$S, T, U \subset G, \qquad S = \{s_1, \ldots, s_n\}, \quad T = \{t_1, \ldots, t_n\}, \quad U = \{u_1, \ldots, u_n\}$$

$$\forall_{i,j,k,l}: \quad s_i t_j^{-1} t_k u_l^{-1} = s_i u_l^{-1}$$

$$\mathbb{C}[G] \cong \mathbb{C}^{d_1\times d_1} \times \ldots \times \mathbb{C}^{d_r\times d_r}$$

Multiplicative rank of multiplication in GF(q^n) over GF(q):

(Chudnovsky brothers'88; S. Ballet, R. Rolland etc. ...)

$$GF(q^n) \xrightarrow{lin} G \cong (GF(q)^r, \otimes), \qquad r = O(n)$$