
Complexity Theory in the Service of Algorithm Design

Erich Kaltofen

Rensselaer

Rensselaer Polytechnic Institute
Department of Computer Science
Troy, New York, USA
Outline

• **Wiedemann’s sparse linear system solver**
  ◦ Coordinate recurrences
  ◦ More applications of the transposition principle

• **Reverse mode of automatic differentiation**
  ◦ Transposition principle by derivatives
  ◦ More applications

• **Polynomial factorization**
  ◦ Berlekamp’s polynomial factorization algorithm
  ◦ use of the Wiedemann method
  ◦ new baby step/giant step algorithm
A “black box” matrix is an efficient procedure with the specifications

\[
\begin{align*}
  y & \in \mathbb{F}^n \\
  B \cdot y & \in \mathbb{F}^n
\end{align*}
\]

\(B \in \mathbb{F}^{n \times n}\)
\(\mathbb{F}\) an arbitrary field

i.e., the matrix is not stored explicitly, its structure is unknown.

Main algorithmic problem: How to efficiently solve a linear system with a black box coefficient matrix?
Idea for Wiedemann’s algorithm

\[ B \in \mathbb{F}^{n \times n}, \mathbb{F} \text{ a (possibly finite) field} \]

\[ \phi^B(\lambda) = c'_0 + c'_1 \lambda + \cdots + c'_m \lambda^m \in \mathbb{F}[\lambda] \text{ minimum polynomial of } B: \]

\[ \forall u, v \in \mathbb{F}^n: \forall j \geq 0: u^{\text{tr}} B^j \phi^B(B)v = 0 \]

\[ \iff \]

\[ c'_0 \cdot u^{\text{tr}} B^j v + c'_1 \cdot u^{\text{tr}} B^{j+1} v + \cdots + c'_m \cdot u^{\text{tr}} B^{j+m} v = 0 \]

\[ \iff \]

\[ \{a_0, a_1, a_2, \ldots\} \text{ is generated by a linear recursion} \]
Theorem (Wiedemann 1986): For random $u, v \in \mathbb{F}^n$, a linear generator for $\{a_0, a_1, a_2, \ldots\}$ is one for $\{I, B, B^2, \ldots\}$.

\[ \forall j \geq 0: c_0a_j + c_1a_{j+1} + \cdots + c_da_{j+d} = 0 \]

\[ \downarrow \text{(with high probability)} \]

\[ c_0B^jv + c_1B^{j+1}v + \cdots + c_dB^{j+d}v = 0 \]

\[ \downarrow \text{(with high probability)} \]

\[ c_0B^j + c_1B^{j+1} + \cdots + c_dB^{j+d} = 0 \]

that is, $\phi^B(\lambda)$ divides $c_0 + c_1\lambda + \cdots + c_m\lambda^m$
Algorithm Homogeneous Wiedemann

Input: $B \in \mathbb{F}^{n \times n}$ singular
Output: $w \neq 0$ such that $Bw = 0$

Step W1: Pick random $u, v \in \mathbb{F}^n$; $b \leftarrow Bv$;
for $i \leftarrow 0$ to $2n - 1$ do $a_i \leftarrow u^\text{tr} B^i b$.
(Requires $2n$ black box calls.)

Step W2: Compute a linear recurrence generator for $\{a_i\}$,
$c_\ell \lambda^\ell + c_{\ell+1} \lambda^{\ell+1} + \cdots + c_d \lambda^d, \quad \ell \geq 0, d \leq n, c_\ell \neq 0$,
by the Berlekamp/Massey algorithm.

Step W3: $\hat{w} \leftarrow c_\ell v + c_{\ell+1} Bv + \cdots + c_d B^{d-\ell} v$;
(With high probability $\hat{w} \neq 0$ and $B^{\ell+1} \hat{w} = 0$.)
Compute first $k$ with $B^k \hat{w} = 0$; return $w \leftarrow B^{k-1} \hat{w}$. 
Steps W1 and W3 have the same computational complexity

\[ u^{\text{tr}} \cdot \begin{bmatrix} v & Bv & B^2v & \ldots & B^{2n}v \end{bmatrix} = \begin{bmatrix} a_{-1} & a_0 & a_1 & \ldots & a_{2n-1} \end{bmatrix} \]

\[ \begin{bmatrix} v & Bv & B^2v & \ldots & B^{2n}v \end{bmatrix} \cdot \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2n} \end{bmatrix} = w \]

**Fact:** \( X \cdot y \) and \( X^{\text{tr}} \cdot z \) have the same computational complexity [Kaminski et al., 1988].