Tutorial 5

1 Wiedemann's algorithm

Let K be a finite field (e.g. $\mathbb{Z}/p\mathbb{Z}$ with p prime) and $M \in M_n(K)$ be an invertible matrix, with $\omega(M)$ non zero coefficients.

1. Recall the main steps of Wiedemann's algorithm to compute a solution of $Mx = b$ for some vector b. What is its complexity ?
2. Assume now that M is non invertible and that its minimal polynomial is known. Can you describe some non-zero vectors in its kernel?
3. Deduce a probabilistic algorithm that finds a non zero element in $\ker M$. What complexity do you obtain ? Compare it with the approach using Gaussian elimination.
4. Propose a modification to Wiedemann's algorithm for a non-square $M \in K^{n\times r}$ for $r < n$.

2 Cauchy matrices

Let $\mathrm{a} = (a_i)_{0\leqslant i\leqslant n-1} \in K^n, \mathrm{b} = (b_i)_{0\leqslant i\leqslant n-1} \in K^n$. We assume that $a_i \neq b_j$ for all i, j and that $a_i \neq a_j$ and $b_i \neq b_j$ for $i \neq j$. The Cauchy matrix associated to these n-tuples is the matrix $C(\mathrm{a}, \mathrm{b}) = (1/(a_i - b_j))_{0\leqslant i,j\leqslant n-1}$. The goal of this exercise is to find H, the inverse of C.

1. Let $A_i(x) = \frac{A(x)}{A'(a_i)(x-a_i)}, B_i(x) = \frac{B(x)}{B'(b_i)(x-b_i)}$ be the fundamental polynomials of the Lagrangian interpolation with $A(x) = \prod_i (x - a_i), B(x) = \prod_i (x - b_i)$. Prove that

$$h_{i,j} = (a_j - b_i) \cdot A_j(b_i) \cdot B_i(a_j).$$

   In case C is symmetric, prove that

$$h_{i,j} = (a_j - b_i) \cdot A_j(b_i) \cdot A_i(b_j).$$

2. Conclude on the complexity of computing H.

3 Quasi-Cauchy matrices

Let $\mathrm{w} := (w_0, \ldots, w_j)$. We define a $j \times j$ diagonal matrix $D(\mathrm{w})$ by

$$D(\mathrm{w}) = \begin{bmatrix} w_0 & 0 & \cdots & 0 \\ 0 & w_1 & \ddots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & w_{j-1} \end{bmatrix}.$$

Let now $\varphi_{\mathbf{x},\mathbf{y}} : \mathcal{M}_n(K) \to \mathcal{M}_n(K)$ defined by $\varphi_{\mathbf{x},\mathbf{y}}(A) = D(\mathbf{x}) \cdot A - A \cdot D(\mathbf{y})$. With these notations, define the $(\mathbf{x}, \mathbf{y})$-displacement rank of A to be the rank of $\varphi_{\mathbf{x},\mathbf{y}}(A)$. We shall assume that $\varphi_{\mathbf{x},\mathbf{y}}(A)$ is an invertible mapping – an easy fact, the proof of which is of little interest.

1. What is the $(\mathbf{x}, \mathbf{y})$-displacement rank of the Cauchy matrix $C(\mathbf{x}, \mathbf{y})$?

2. Let $\mathbf{u}, \mathbf{v}$ be two (column) vectors in K^n. Prove that $\varphi^{-1}_{\mathbf{x},\mathbf{y}}(\mathbf{u} \cdot {}^t\mathbf{v}) = D(\mathbf{u})C(\mathbf{x}, \mathbf{y})D(\mathbf{v})$.

3. Deduce from the previous question that if a matrix M has $(\mathbf{x}, \mathbf{y})$-displacement rank α, there exist vectors $\mathbf{g}_1, \ldots, \mathbf{g}_\alpha, \mathbf{h}_1, \ldots, \mathbf{h}_\alpha$ such that

$$M = \sum_{j=1}^{\alpha} D(\mathbf{g}_j)C(\mathbf{x}, \mathbf{y})D(\mathbf{h}_j). \tag{1}$$

   (Hint: recall that if N has rank α, then $N = \sum_{i=1}^{\alpha} N_i$ with N_i of rank 1.)

4. Prove conversely that if M is of the form (1), then M has $(\mathbf{x}, \mathbf{y})$-displacement rank $\leqslant \alpha$.

   For the rest of the exercise, we shall say that a matrix with $(\mathbf{x}, \mathbf{y})$-displacement rank α is represented by $(\mathbf{x}, \mathbf{y})$-generators of size α if M is given as a pair of vector sequences $((\mathbf{g}_i)_{1 \leqslant i \leqslant \alpha}, (\mathbf{h}_i)_{1 \leqslant i \leqslant \alpha}) \in (K^\alpha)^2$ such that (1) holds. Overall, this means that, when α is small, we have a compact representation for M (of size $O(\alpha n)$), and we might wonder whether we can do basic matrix arithmetic – matrix/vector product, add, multiply, inverse, determinant – using this compact representation (the last two can be done but we'll not study them).

5. If M is represented by $(\mathbf{x}, \mathbf{y})$-generators of size α and v is a vector, prove that one can compute $M \cdot v$ in complexity $O(\alpha M(n) \log n)$.

6. If M, M' are represented by $(\mathbf{x}, \mathbf{y})$-generators of size α and α', give $(\mathbf{x}, \mathbf{y})$-generators of size $\alpha + \alpha'$ for $M + M'$, which can be computed in time $O((\alpha + \alpha')n)$.

7. If M, M' are represented by $(\mathbf{x}, \mathbf{y})$-generators of size α (resp. by $(\mathbf{y}, \mathbf{z})$-generators of size α'), give $(\mathbf{x}, \mathbf{y})$-generators of size $\alpha+\alpha'$ for $M \cdot M'$, which can be computed in time $O(\alpha\alpha' M(n) \log n)$.