TUTORIAL

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 Lanczos algorithm

In this exercise we are going to consider a linear equation

$$Ax = b$$

over the real numbers and we assume we can compute with sufficient precision (i.e., values close to 0 are *not* treated as 0).

1. Show that we can further assume that A is symmetric and positive definite.
2. We thus assume A is symmetric and positive definite. Then, it induces scalar product as

   $$\langle x, y\rangle_A := \langle x, Ay\rangle = \langle Ax, y\rangle$$

   Consider the following orthogonalization process:

   - set $v_0 = b$;
   - for $i \geq 0$, set $w_i = Av_i$ and

   $$v_{i+1} = w_i - \sum_{j=0}^{i} \frac{\langle w_j, v_i\rangle_A}{\langle v_j, v_j\rangle_A} \cdot v_j$$

   Show that this creates indeed an orthogonal family in $\mathbb{R}^n$ w.r.t. A. How many scalar products you need to compute this basis?
3. Show how to compute the solution x in time $O(n^2)$.
4. What might get wrong in the above process?

3 Iterative methods for solving linear systems

In this exercise, we let that $K = \mathbb{R}$ or $K = \mathbb{C}$. We will consider iterative methods to compute an approximation of the solution of a system

$$Ax = b \tag{1}$$

with A an invertible matrix of size n.

1. Let $A = M - N$ with $M, N \in M_n(K)$ and M invertible. Show that solving (1) is equivalent to find a fixed point of the function $f : K^n \to K^n$ defined by $f(x) = M^{-1}Nx + M^{-1}b$.

   We first design an algorithm to compute an approximation of x under some assumptions:

   - we assume that x is the unique fixed point of f;
   - for some known $x_0 \in K$, the sequence defined by $x_{n+1} = f(x_n)$ converges to x.

   In a second part, we will give a sufficient condition for these assumptions.

2. **Jacobi's method:** assume that A has no zero on its diagonal. Show that the next term in the sequence can be computed in $O(n^2)$ operations for a good choice of M, N.

   Further assume that there exists $0 \leq k < 1$ such that, for all $x_1, x_2 \in K^n$, we have $\|f(x_1) - f(x_2)\| \leq k\|x_1 - x_2\|$. Such a map is called *a contraction*.

3. Give an algorithm to compute an approximation of x such that $Ax = b$ with at least r bits of precision for each coordinate. What is its complexity in terms of operations in K (assume we already know a ball of radius 10 containing x)?

   We now give general examples of contractions. Let $M \in M_n(K)$ be a matrix. We define the matrix norm of M associated to $\|.\|$ by

   $$|||M||| = \sup_{x \in K^n \setminus \{0\}} \left(\frac{\|Mx\|}{\|x\|} \right).$$

4. Prove that $|||M||| = \max_{x \in K^n, \|x\|=1} (\|Mx\|)$ (beware, there is now a max and not a sup). (Hint: use the fact that the unit ball is compact in K^n).

5. Let f be as in question 1, and give a condition on M and N such that f is a contraction.

6. Let A be a strictly row diagonally dominant matrix, that is $|a_{i,i}| > \sum_{j \neq i} |a_{i,j}|$ for all $1 \leq i \leq n$. Prove that the Jacobi's method converges for A (Hint : use the $\| \cdot \|_\infty$ norm to prove that the condition of question 5 is satisfied).

   Banach-Picard's fixed point theorem : we now show that the "contraction" assumption implies the two others.

7. Let $g : K^n \to K^n$ be a contraction. Prove that g has at most one fixed point ℓ in K^n.

8. Let $x_0 \in K^n$ be any vector and define $x_{n+1} = g(x_n)$. Prove that this sequence converges. What is its limit ? What is the speed of convergence of this sequence ?