Prof. Friedrich Eisenbrand
Yuri Faenza

Discussions from: April 09, 2013

Computer Algebra

Spring 2013

Assignment Sheet 4

Exercises marked with a $\star$ can be handed in for bonus points. Due date is April 23.

Exercise 1

Recall the *Sieve of Eratosthenes*, that detects which integers smaller or equal to an input n are prime (at the end of the algorithm, a number $t \in [2, n]$ is prime iff $A[t] = 1$).

```
INPUT: integer n ∈ ℕ,   OUTPUT: vector A[2,...,n].

FOR k = 2 to n SET A[k] = 1
FOR k = 2 to ⌊n/2⌋

    IF A[k] = 1
        SET i = 2k
        WHILE i ≤ n
            SET A[i] = 0
            SET i = i + k

    RETURN A[2,...,n]
```

a) *Merten's Theorem* is the following result: for each $n \in \mathbb{N}$, $\sum_{p \leq n:\, p \text{ is a prime}} \frac{1}{p} = \log(\log n) + O(1)$. Assuming the previous, show that the running time of the Sieve of Eratosthenes is $O(n \log(\log n))$.

b) Implement the sieve of Eratosthenes.

Exercise 2

Show the following: for each $\epsilon > 0$, there exists $c \in \mathbb{R}_+$, $N \in \mathbb{N}$ such that, for each $n \geq N$, one has $\pi((1+\epsilon)n) - \pi(n) \geq c\frac{n}{\log n}$, where for $n \in \mathbb{N}$ we have $\pi(n) = \{p \leq n : p \text{ is prime}\}$.

Exercise 3

Let $A \in \mathbb{Q}^{n \times n}$. Denote the columns of A by $a_1, \ldots, a_n$. Let B be an upper bound on the absolute values of entries in A.

1. Show the Hadamard bound $|\det(A)| \le \prod_{j=1}^{n} |a_j|_2$, where $|\cdot|_2$ is the Euclidean norm.

   Hint: Do you remember the Gram-Schmidt orthogonalization process?

2. Derive from this that $|\det(A)| \le n^{n/2} B^n$. Leibniz formula states that $|\det(A)| \le B^n n!$. How does it compare to Hadamard bound?

Exercise 4 ($\star$)

Show that, using Gaussian elimination, one can compute a solution to the system $Ax = b$, $A \in \mathbb{Q}^{m\times n}$, $b \in \mathbb{Q}^m$, or assert that none exists, in polynomial time in the encoding length of A and b.

Exercise 5

Let $M \in \mathbb{R}^{m\times n}$, and M' be the matrix obtained after performing an elementary row operation on M.

a) Show that there exists an invertible matrix X such that $M' = XM$.

b) Let B be the output of Gaussian elimination when applied to A. From *a*), one immediately checks that $B = XA$ for some invertible matrix X. Modify the Gaussian elimination algorithm as to compute X.

Exercise 6

Let

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

1. Use Gaussian elimination modulo p to compute the determinant of A modulo p, for $p = 3, 5, 7$.

2. Use the Leibniz bound to show that $2|\det(A)| + 1 \le 105$. Conclude that you can directly obtain $\det(A)$ from the previous results.

Exercise 7

Let $T(G)$ be the Tutte matrix of a graph G, and $\nu(G)$ the cardinality of the maximum matching of G.

a) Given a graph G, show that there exists a subgraph H of G with a perfect matching such that $2\nu(G) = 2\nu(H) = \mathrm{rank}(T(H)) = \mathrm{rank}(T(G))$[1].

b) Give an efficient randomized algorithm that computes the cardinality of a maximum matching of a graph with probability at least $1/2$.

[1] Note that this does not immediately implies that we can compute $\nu(G)$, because we still have to show how to compute the rank of a matrix with indeterminate entries.