Randomized Algorithms
Assignment 6 - Resubmission

Nikolaj Dybdahl Rathcke (rfq695)
Victor Petren Bach Hansen (grn762)

June 10, 2016

Problem 1

TODO

Problem 7.4

Let us construct the polynomial $P_1(x)$ and $P_2(x)$ in the following way:

$$P(x) = \prod_{i=1}^{n}(x - e_i)$$

where e_i are the elements belonging to set S_1 and S_2. Now let us consider the difference polynomial $Q(x) = P_1(x) - P_2(x)$. Now we know that $Q(x)$ is equivalent to 0 only when $S_1 = S_2$ as polynomials are unique given their factorization. Now, Q has degree d, meaning there are at most d (distinct) roots. We can upper bound d by n, meaning if we pick an element $r \in [0, n^2]$, we can use Theorem 7.2 to verify they are different with probability at least $1 - 1/n$, which is also the error probability for a false positive. Obviously, the integers can be huge in this verification algorithm, which means it can be computationally hard to evaluate. The verification where the sets are sorted does not suffer from this. However, we can use the fingerprinting techniques picking an appropiate prime p, which will limit the probability that p is a root in $Q(x)$ to $1/2$. It will, however, allow us to evaluate Q in linear time, which means it is faster than the sorting verification algorithm.
If we use the logarithmic-cost RAM model instead of the unit-cost though, we will also have a running time of $\mathcal{O}(n \lg n)$ as well due to the multiplications in which case most people would probably prefer a deterministic algorithm instead!