

CS 3233 Midterm I Review

Practice Problems

Chapter 1

Key Terms and Results (pp. 111–113): all Logic terms except for “free variable”, all Methods of Proof term except “constructiv existence proof” through “uniqueness proof”, all Set terms except for “membership table”, all Function terms except “ $f \circ g$ (composition of f and g)”.

Review Questions (pp. 113–114): 1a, 2a, 4a, 4c with truth tables, 6–9, 11, 14, 15, 17a, 18, 20, 22.

Supplementary Exercises (pp. 114–116): 2, 3, 5, 11, 14–17, 16, 34–46. 47ab, 50–52.

Chapter 2

Key Terms and Results (pp. 206–207): the terms from “algorithm” to “sorting”, “ $O(g(x))$ ”, “time complexity” to “composite”, “ $\gcd(a,b)$ ”, “ $a \bmod b$ ”, “base b representation” to “octal representation”, “matrix” to “matrix multiplication”, “zero-one matrix”, and “Boolean product”. For results, see algorithms in class notes.

Review Questions (pp. 208–209): 1–4, 6–8, 12acd, 14 (convert decimal to binary), 21, 22.

Supplementary Exercises (pp. 209–210): 1–5, 8, 13, 14, 16, 23–25, 35, 42.

An Aside

Here is how to find large prime numbers (with high probability).

If a number n is prime, then $a^{n-1} \bmod n = 1$ for any a when $2 \leq a \leq n - 1$ (see Theorem 5 in Section 2.6). If a number n is not prime, it turns out that $a^{n-1} \bmod n \neq 1$ for at least half of the numbers between 2 and $n - 1$. This justifies the algorithm due to Miller and Rabin.

procedure *prime_test*(n, s : positive integers)

```
  for  $i := 1$  to  $s$ 
     $a :=$  a random integer between 2 and  $n - 1$ 
    if  $a^{n-1} \bmod n \neq 1$  then return false
  return true
```

s is the number of times n is tested. If s is 20, the chance that a true answer is wrong is less than 1 in a million. Of course, we had better have an efficient algorithm to compute $a^{n-1} \bmod n$.

It turns out that the density of primes about a number n is about $1/(\log n)$, i.e., about 1 out of every $\log n$ numbers around n are prime. If random numbers are sampled from a large region, a prime should soon be found.