# Written exam – mock exam

Name: ..................................

Data structures and algorithms (GEMAK117-MA)

June 3, 2024

Neptun code: ..........................

## Part 1: theoretical questions (20 points)

I will ask a few definitions and theorems and one algorithm – from the UPDATED glossary, now containing material on graphs as well.

**Exercise 1** (9 points)**.** State the following definitions (1 point each):

a) whole quotient, div operation

$a \text{ div } b = \left\lfloor \frac{a}{b} \right\rfloor$

b) small $o$ notation

$f$ and $g$ are functions on $\mathbb{N}$. $f(n) = o(g(n))$ if $\dfrac{f(n)}{g(n)} \to 0$ as $n \to \infty$.

c) algorithm

a step-by-step calculation to solve a problem

d) Fibonacci numbers

a number sequence defined recursively: $F_0 = 0$, $F_1 = 1$, then $F_n = F_{n-1} + F_{n-2}$.

e) prime

$p > 1$ is a prime if it is only divisibly by 1 and itself.

f) congruence

$a \equiv b \mod n$, if $a$ and $b$ have the same remainder when divided by $n$.

g) multiplicative inverse

$a^{-1} \mod n$ only exists when $\gcd(a, n) = 1$. Then it's the single solution $x \in [0, n)$ of the linear congruence equation $ax \equiv 1 \mod n$.

h) directed graph

$G = (V, E)$, where $V$ is a finite set, set of vertices, $E$ is a set of ordered pairs from $V$, set of edges

i) path (in a graph)

sequence of connecting edges that don't cross the same vertex twice

**Exercise 2** (8 points)**.** State the following theorems (2 points each):

a) reduction theorem (of the greatest common divisor)

$a$ and $b$ are whole numbers. $\gcd(a, b) = \gcd(a - b, b)$.

b) number of digits (in base $b$)

$x$ positive, whole number has $\lfloor \log_b(x) \rfloor + 1$ digits in base $b$.

c) the “master theorem”

given a recursive equation $T(n) = aT\left(\frac{n}{b}\right) + f(n)$.

suppose $a \geq 1, b > 1$, $f$ is a function $\mathbb{N} \to \mathbb{R}^+$.

define $p = \log_b(a)$, $g(n) = n^p$ test polynomial.

a) if $f(n)$ grows polynomially slower than $g(n)$, then $T(n) = \Theta\big(g(n)\big)$.

b) if $f(n) = \Theta(g(n))$, then $T(n) = \Theta\big(g(n) \cdot \log(n)\big)$.

c) if $f(n)$ grows polynomially faster than $g(n)$, and also $f(n)$ satisfies regularity:

for some $c < 1$, $c \cdot f(n) \leq af\left(\frac{n}{b}\right)$,

then $T(n) = \Theta\big(f(n)\big)$.

d) lower bound on comparison-based sorting

for a comparison-based sorting algorithm, at least $\Omega\big(n\log(n)\big)$ comparisons are needed

**Exercise 3** (3 points)**.** Write down the algorithm for **modular exponentiation**.

**MOD_EXP**(a,b,n,@c)
// INPUT: whole numbers a,b,n
// OUTPUT: $c = (a^b \mod n)$
write the exponent $b$ in base 2: $b_n b_{n-1} \dots b_1 b_{0(2)}$
$c \leftarrow 1$
FOR k ← n DOWNTO 0 DO // that is: read binary digits of $b$ left to right
    $c \leftarrow c^2 \mod n$
    IF $b_k = 1$ THEN
        $c \leftarrow c \cdot a \mod n$
**RETURN**(c)

Part 2: exercises (20 points)

I will pick 4 exercises from 8 possible types, 5 points per exercise. Possible exercise types: 6 already known from the practical midterm (you can find worked out exercises of each type in the lecture notes) + 2 new types: linear congruence equation and Dijkstra algorithm. Only showing new types and their solutions below:

**Exercise 4** (Linear congruence equation)**.**

- variant 1: “Solve the linear congruence equation $4x \equiv 2 \mod 10$.”

  step 1: calculate $\gcd(a, n) = \gcd(4, 10)$ – Euclidean algorithm (just the green part of the table yet)

| i | n | a | q | r | $y^\star$ | $x^\star$ |
|---|---|---|---|---|---|---|
| 0 | 10 | 4 | 2 | 2 | 1 | $0 - 1 \cdot 2 = -2$ |
| 1 | 4 | 2 | 2 | 0 | 0 | $1 - 0 \cdot 2 = 1$ |
| 2 | 2 | 0 | | | 1 | 0 |

$d = \gcd(10, 4) = 2$.

step 2: check if $d$ divides $b = 2$ (right hand side of congruence). $d = 2|2 = b$, OK! (if $d$ does not divide $b$, no solutions.) means there should be $d = 2$ basic solutions, meaning solutions $0 \leq x < n = 10$.

step 3: find basic solutions. for this, we need coefficient $x^\star$ from the linear combination $d = x^\star a + y^\star n$. go back to the table of Euclidean algorithm, and finish the extended Euclidean algorithm! (right hand side of the table, in red above)

we get $x^\star = -2$.

the special solution: $x_0 = x^\star \cdot \frac{b}{d^\star} \mod n = -2 \cdot \frac{2}{2} \mod 10 = -2 \mod 10 = 8$.

the other solutions (now just 1 more):

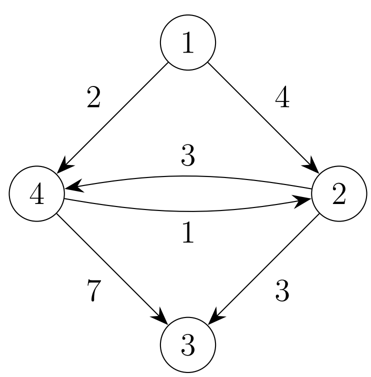
$x_i = x_0 + i \cdot \frac{n}{d^\star} \mod n, \quad i = 1, 2, \ldots, d^\star - 1$

$x_1 = 8 + 1 \cdot \frac{10}{2} \mod 10 = (8 + 5) \mod 10 = 13 \mod 10 = 3$.

- variant 2: "Calculate the multiplicative inverse $x = 8^{-1} \mod 11$."

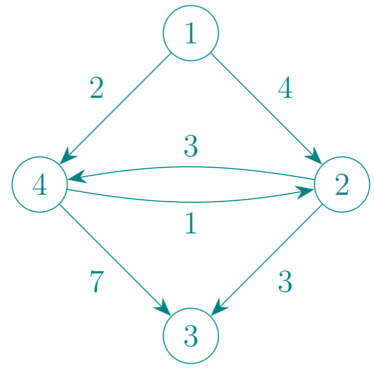
  basically: by definition of multiplicative inverse, this means: solve linear congruence equation $8x \equiv 1 \mod 11$. see the solution above. – it should be true that $\gcd(8, 11) = 1$, and there's only 1 basic solution, the special solution $x_0$.

**Exercise 5** (Dijkstra algorithm)**.** Find the shortest paths using Dijkstra's algorithm from source $s = 1$ in the following graph:

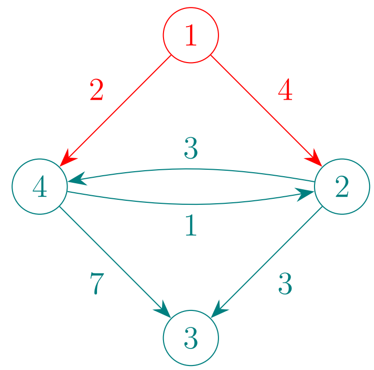


0) initially: $S = \{\}$ (empty set), $Q = \{1, 2, 3, 4\}$,
since $s = 1$, $d = [0, \infty, \infty, \infty]$, $\pi =$ [NIL,NIL,NIL,NIL].

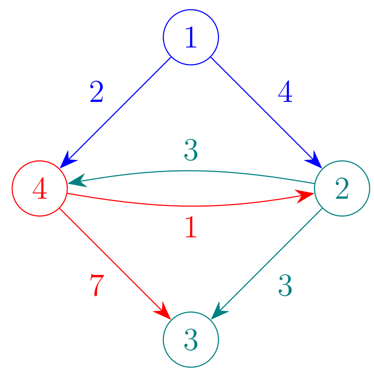
color coding below:
in $d$ and $\pi$: finalized values, freshly updated values.
in drawing: $u$ and its outgoing edges; vertices already in $S$ (and their outgoing edges)



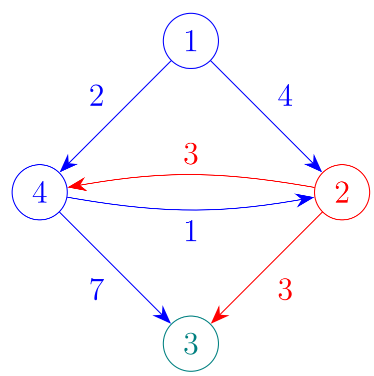

1) pick $u$ from $Q$ (still green/red) with smallest $d[u]$: $u = 1$. move $u$ to $S$ and update with all edges going out of $u$ (see if we can get a shorter path to vertices in $Q$ through these edges):
$S = \{1\}$, $Q = \{2, 3, 4\}$,
$0 + 4 < \infty$, $0 + 2 < \infty$: reach 2 and 4 from vertex 1.
$d = [0, 4, \infty, 2]$, $\pi =$ [NIL,1,NIL,1].



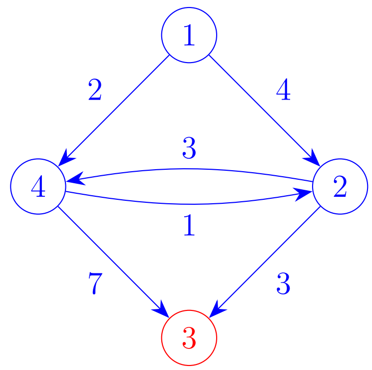

2) again, pick $u$ from $Q$ (still green/red) with smallest $d[u]$: $u = 4$. move $u$ to $S$ and update with all edges going out of $u$:
$S = \{1, 4\}$, $Q = \{2, 3\}$,
$2 + 1 < 4$, $2 + 7 < \infty$: reach 2 and 3 through 4
$d = [0, 3, 9, 2]$, $\pi =$ [NIL,4,4,1].



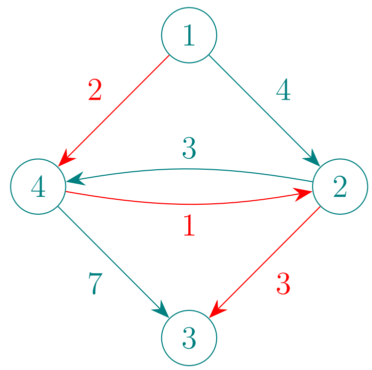

3) repeat...
$u = 2$.
$S = \{1, 2, 4\}$, $Q = \{3\}$,
$3 + 3 < 9$
$d = [0, 3, 6, 2]$, $\pi =$ [NIL,4,2,1].



4) repeat...
$u = 3$.
$S = \{1, 2, 3, 4\}$, $Q = \{\}$,
(no outgoing edges to update with.)
$d = [0, 3, 6, 2]$, $\pi =$ [NIL,4,2,1].




5) $Q$ is empty, we are done!
final result: $d = [0, 3, 6, 2]$, $\pi =$ [NIL,4,2,1].
read shortest paths: highlight $(\pi[u], u)$ edges in red:
(NIL,1) – not an edge, no highlight; (4,2), (2,3), (1,4)




Scoring

- total: 40 points
- 20 points- : 2 (sufficient)
- 24 points- : 3 (mediocre)
- 28 points- : 4 (good)
- 32 points- : 5 (excellent)