ITB8832 Mathematics for Computer Science
Final Exam, first date: 20 December 2023

Last update: 21 December 2023

Exercise 1 (8 points)

Four men and four women have the following lists of preferences:

Cloud	Aerith, Tifa, Yuna, Rinoa	Aerith	Tidus, Zack, Squall, Cloud
Squall	Yuna, Rinoa, Aerith, Tifa	Rinoa	Cloud, Squall, Tidus, Zack
Tidus	Tifa, Yuna, Rinoa, Aerith	Tifa	Squall, Cloud, Zack, Tidus
Zack	Rinoa, Aerith, Tifa, Yuna	Yuna	Zack, Tidus, Cloud, Squall

1. (4 points) Prove that the matching:

   (Cloud, Tifa), (Squall, Rinoa), (Tidus, Yuna), (Zack, Aerith)

   is stable.

2. (4 points) Prove that this matching cannot have been produced by the Mating Ritual.

Exercise 2 (10 points)

A certain subset M of the set of natural numbers $\mathbb{N}$ is defined recursively as follows:

- **Base case:** $2 \in M$.
- **Constructor case 1:** for every $n \in \mathbb{N}$, if $n \in M$ then $2n \in M$.
- **Constructor case 2:** for every $n \in \mathbb{N}$, if $n \in M$ and $n \geq 1$ then $n - 1 \in M$.

Your tasks for this exercise:

1. (1 point) Explain why the definition of M given in the text is ambiguous.

2. (3 points) Prove that $M = \mathbb{N}$. *Hint:* you do *not* need induction to solve this point.

3. (6 points) Let now a be a positive real number and let $f : M \to M$ be defined recursively as follows:

   - **Base case:** $f(2) = a$.
   - **Constructor case 1:** for every $n \in \mathbb{N}$, $f(2n) = (f(n))^2$.
   - **Constructor case 2:** for every $n \in \mathbb{N}$, if $n \geq 1$ then $f(n-1) = f(n)/\sqrt{a}$.

   Prove by structural induction that $f(n) = a^{n/2}$ for every $n \in M$.

Exercise 3 (10 points)

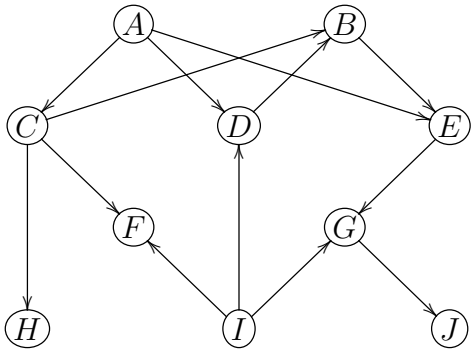
Let $p = 97$ and $q = 41$.

1. (3 points) Prove that $(e, n) = (343, 3977)$ is a valid RSA public key.

2. (7 points) Determine the private key d for the public key (e, n) of the previous point .

Exercise 4 (12 points)

The following directed acyclic graph D represents a list of tasks together with their priorities:



In addition to D, consider the simple graph G with the same set of vertices as D, and where $\langle u—v \rangle$ is an edge in G if and only if one between $\langle u \to v \rangle$ and $\langle v \to u \rangle$ is an edge in D.

1. (3 points) Construct a parallel schedule of minimum time for the set of tasks described by D, in the hypothesis that every task requires one unit of time.

2. (1 point) Does this set of tasks have a parallel schedule of minimum time with only two processors?

   This point is considered as solved if the schedule in your answer to point 1 uses only two processors.

3. (1 point) Draw a spanning tree of G.

4. (3 points) Prove that the chromatic number of G is 3.

5. (4 points) Prove that G is not planar. *Hint:* $K_{3,3}$.

Exercise 5 (20 points overall)

For each of the following questions, mark the only correct answer:

1. Which one of the following numbers is irrational?

   (a) $\log_{16} 512$.

   (b) $\log_2 32$.

   (c) $\log_2 31$.

2. Which one of the following subsets of $\mathbb{R}$ is well ordered?

   (a) $A ::= \left\{ \frac{n}{2^n} \mid n \in \mathbb{N} \right\}$.

   (b) $B ::= \left\{ \frac{n+1}{n+2} \mid n \in \mathbb{N} \right\}$.

   (c) $C ::= \left\{ \frac{n+2}{n+1} \mid n \in \mathbb{N} \right\}$.

3. Which one of the following propositional formulas is valid?

   (a) $((P$ **implies** $Q)$ **and not**$(Q))$ **iff** P.

   (b) $((P$ **implies** $Q)$ **and** $Q)$ **implies** P.

   (c) $((P$ **implies** $Q)$ **and** $P)$ **implies** Q.

4. True or false: the predicate formula $\forall x \,.\, \exists y \,.\, P(x, y)$ has a counter-model.

5. Which one of the following is a preserved invariant for the Die Hard machine with jugs of 30 and 24 liters?

   (a) ℓ is a multiple of 8.

   (b) ℓ is a multiple of 6.

   (c) ℓ and b are both multiples of 6.

6. Consider the Mating Ritual for n men and n women with men as suitors. Which one of the following statements is true?

   (a) If a woman has a suitor on one evening, then she has a suitor on every following evening.

   (b) If a woman has a suitor on one evening, then she has the same suitor on every following evening.

   (c) If a man has a woman on his list on one morning, then he has her on his list on every following morning.

7. Which one of the following functions is correctly defined by recursion for every $n \in \mathbb{N}$?

   (a) $f(n) ::= n + 3f(n-1)$ for every $n \geq 1$.

   (b) $g(n) ::= \dfrac{n}{g(n-1)}$ for every $n \geq 1$, $g(0) ::= 1$.

   (c) $h(n) ::= \dfrac{n}{(n-1)h(n-1)}$ for every $n \geq 1$, $h(0) ::= 1$.

8. Which one of the following Nim games is a winning position for the first player?

   (a) $\text{Nim}_{(43,27,48)}$.

   (b) $\text{Nim}_{(33,17,48)}$.

   (c) $\text{Nim}_{(43,17,38)}$.

9. True or false: given any two sets A and B, if both A surj B and B surj A, then A bij B.

10. Which one of the following subsets of ASCII* is recognizable?

    (a) $L ::= \{s \in \text{ASCII}^* \mid \lambda \notin \text{lang}(P_s)\}$.

    (b) $M ::= \{s \in \text{ASCII}^* \mid \text{lang}(P_s) \text{ is finite}\}$.

    (c) $N ::= \{s \in \text{ASCII}^* \mid \texttt{01}s\texttt{10} \in \text{lang}(P_s)\}$.

11. What is the remainder in the division of $10000^{16324864} + 47^{4096}$ by 17?

    (a) 0.

    (b) 1.

    (c) 2.

12. In which one of the following cases a total function $f : \mathbb{Z}^+ \to \mathbb{C}$ is multiplicative?

    (a) $f(m \cdot n) = f(m) \cdot f(n)$ for every $m, n \in \mathbb{Z}^+$.

    (b) $f(m \cdot n) = f(m) \cdot f(n)$ for every $m, n \in \mathbb{Z}^+$ such that $\gcd(m, n) = 1$.

    (c) $f(m \cdot n) = f(m) \cdot f(n)$ for every $m, n \in \mathbb{Z}^+$ such that $\operatorname{lcm}(m, n) = 1$.

13. Let (e, n) be an RSA public key. Which one of the following would allow us to efficiently reconstruct the private key d?

    (a) Efficiently factoring a product of two primes.

    (b) Efficiently calculating $d^e \pmod{n}$.

    (c) Efficiently determining if n is prime.

14. True or false: in every finite directed graph, the sum of the in-degrees of the vertices is equal to twice the number of the edges.

15. Which one of the following is true for every directed acyclic graph D on 96 vertices?

    (a) D has a chain of size 8.

    (b) D has either a chain of size 8 or an antichain of size 14, and possibly both.

    (c) D has either a chain of size 8 or an antichain of size 14, but not both.

16. Which one of the following is true?

    (a) Every linear order is a weak partial order.

    (b) Every strict partial order is a weak partial order.

    (c) Every strict partial order is the walk relation of a DAG.

17. Which one of the following binary relations on the set of real numbers is a weak partial order?

    (a) $x \, R \, y$ **iff** $x - y > 0$.

(b) $x\,S\,y$ **iff** $\lceil x \rceil \leq \lceil y \rceil$.

(c) $x\,T\,y$ **iff** $2^x \leq 2^y$.

18. What is a matching in a simple graph G?

    (a) A subset M of the set E of the edges of G such that every vertex of the graph is an endpoint of an edge in M.

    (b) A subset M of the set E of the edges of G such that every vertex of the graph is an endpoint of at most one edge in M.

    (c) A subset M of the set E of the edges of G such that every vertex of the graph is an endpoint of at least one edge in M.

19. True or false: A simple graph with 47 vertices, 51 edges, and 3 connected components must contain a cycle.

20. Which one of the following simple graphs is planar?

    (a) A connected graph with 17 vertices and 16 edges.

    (b) A graph with 17 vertices and 46 edges.

    (c) A bipartite graph with 17 vertices and 36 edges.

This page intentionally left blank.

This page too.

Solution

Exercise 1

1. Every person is matched to their own second choice and is the last choice of their own first choice. Then there cannot be rogue couples, because the only person with which anyone could form a rogue couple, prefer their own spouse to them. For example, Cloud could form a rogue couple only with Aerith, but Aerith prefers her partner Zack to Cloud, and will not form a rogue couple with Cloud. The arguments for the remaining three men and for the four women are similar.

2. Every man has a different first choice and every woman has a different first choice, so the Mating Ritual will produce a stable set of matchings on the first day. If men are suitors, then Cloud will be matched with Aerith, not with Tifa; if women are suitors, then Cloud will be matched with Rinoa, not with Tifa.

Exercise 2

1. 2 is a base case, but we can also obtain it by applying the first constructor with $n = 2$, then applying the second constructor to $n = 4$, then applying the second constructor to $n = 3$. Another example is to obtain 6 as $2 \to 4 \to 8 \to 7 \to 6$ or as $2 \to 4 \to 3 \to 6$.

2. An argument that does not use induction is the following. Let $n \in \mathbb{N}$ and let $m \geq 1$ be the number of bits in its binary writing. Then $2^m > n$, so we can obtain n by starting from 2, then applying the first constructor $m - 1$ times (possibly never) to obtain 2^m, then applying the second constructor $2^m - n$ times to obtain n.

   An argument by induction considers the predicate $P(n) ::= n \in M$ and proves the predicate formula $\forall n \in \mathbb{N} \,.\, P(n)$ as follows:

   - **Base case:** $n = 0$. We can obtain 0 by starting from 2, then applying the second constructor to obtain 1, then applying the second constructor to 1 to obtain 0. We conclude that $P(0)$ is true.
   - **Inductive step:** Assume that a certain natural number n is an element of M. We want to prove that $n + 1 \in M$ too. We must distinguish two cases:
     (a) $n = 0$. Then $n + 1 = 1$ can be obtained by applying the second constructor to the base case 2.

(b) $n \geq 1$. Then $2n \geq n+1 \geq 2$, and we can obtain $2n$ by applying the first constructor to n, which is an element of M by inductive hypothesis. After we have done so, by applying the second constructor $n-1$ times starting from $2n$, we obtain $n+1$.

We have proved that if $P(n)$ is true for a certain $n \in \mathbb{N}$, then $P(n+1)$ is also true for the same n. As we didn't make any special hypothesis on n except that it is a natural number, we conclude that the predicate formula $\forall n \in \mathbb{N}\,.\,(P(n)$ **implies** $P(n+1))$ is true.

3. By structural induction:

   - **Base case:** $n = 2$. Then $f(2) = a = a^{2/2}$.
   - **Constructor case 1:** $n = 2m$ for some $m \in \mathbb{N}$ such that $f(m) = a^{n/2}$. Then:

$$\begin{aligned} f(n) &= f(2m) \\ &= (f(m))^2 \\ &= \left(2^{m/2}\right)^2 = 2^m = 2^{(2m)/2}\,. \end{aligned}$$

   - **Constructor case 2:** $n = m-1$ for some $m \in \mathbb{N}$ such that $m \geq 1$ and $f(m) = 2^m$. Then:

$$f(n) = f(m-1) = \frac{f(m)}{\sqrt{a}} = a^{m/2\,-\,1/2} = 2^{(m-1)/2}\,.$$

Exercise 3

1. The numbers p and q are distinct prims and their product is n. We have $\phi(97) = 96 = 2^5 \cdot 3$ and $\phi(41) = 40 = 2^3 \cdot 5$, so $343 = 7^3$ has a multiplicative inverse modulo $\phi(n) = 96 \cdot 40 = 3840$.

2. To determine the private key, we use the Pulverizer:

a	b	$\text{rem}(a,b)$	$= a - \text{qcnt}(a,b) \cdot b$
3840	343	67	$= 3840 - 11 \cdot 343$
343	67	8	$= 343 - 5 \cdot 67$
			$= 343 - 5 \cdot (3840 - 11 \cdot 343)$
			$= -5 \cdot 3840 + 56 \cdot 343$
67	8	3	$= 67 - 8 \cdot 8$
			$= (3840 - 11 \cdot 343) - 8 \cdot (-5 \cdot 3840 + 56 \cdot 343)$
			$= 41 \cdot 3840 - 459 \cdot 343$
8	3	2	$= 8 - 2 \cdot 3$
			$= (-5 \cdot 3840 + 56 \cdot 343) - 2 \cdot (41 \cdot 3840 - 459 \cdot 343)$
			$= -87 \cdot 3840 + 974 \cdot 343$
3	2	1	$= 3 - 2$
			$= (41 \cdot 3840 - 459 \cdot 343) - (-87 \cdot 3840 + 974 \cdot 343)$
			$= 128 \cdot 3840 - 1433 \cdot 343$

Then the private key is $d = \text{rem}(-1433, 3840) = 2407$.

Exercise 4

1. A schedule of minimum parallel time can be obtained by executing at time t all and only the tasks corresponding to vertices of depth t in D:

$$\begin{aligned} A_0 &= \{A, I\} \\ A_1 &= \{C, D\} \\ A_2 &= \{B, F, H\} \\ A_3 &= \{E\} \\ A_4 &= \{G\} \\ A_5 &= \{J\} \end{aligned}$$

2. The vertex H is maximal and doesn't have maximum depth, so we can postpone it and still get a two-processor parallel schedule of minimum time. For example:

$$\begin{aligned} B_0 &= \{A, I\} \\ B_1 &= \{C, D\} \\ B_2 &= \{B, F\} \\ B_3 &= \{E\} \\ B_4 &= \{G\} \\ B_5 &= \{H, J\} \end{aligned}$$

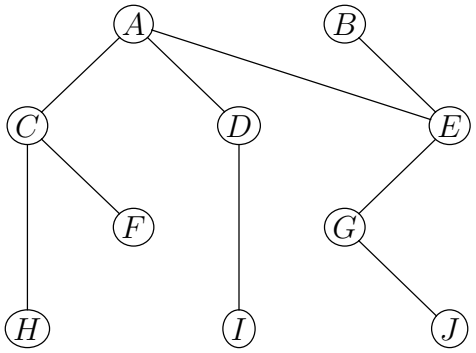


Figure 1: A spanning tree of the graph G of Exercise 4.

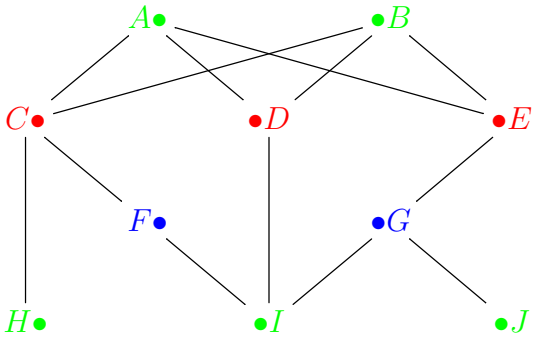


Figure 2: A 3-coloring of the graph G of Exercise 4.

3. There are many options. One is depicture in Figure 1.

4. The simple graph G contains the cycle $ADIFCA$ of length 5, so it is not 2-colorable. A 3-coloring of G is depicted in Figure 2.

5. If we remove from G the vertices H and J and the edges incident on them, we obtain the graph in Figure 3, which is isomorphic to a subdivision of $K_{3,3}$. For example, we could take $L = \{A, B, I\}$ and $R = \{C, D, E\}$ and obtain F by splitting $\langle C—I \rangle$ and G by splitting $\langle E—I \rangle$. We conclude by Kuratowski's theorem that G is nonplanar. Alternatively, merging H with C and J with G, then F with C and G with E, we obtain $K_{3,3}$ as a minor of G: we then conclude by Wagner's theorem that G is not planar.

Exercise 5

1. (a) **No:** $512 = 2^9$ and $16 = 2^4$, so $\log_{16} 512 = 9/4$.

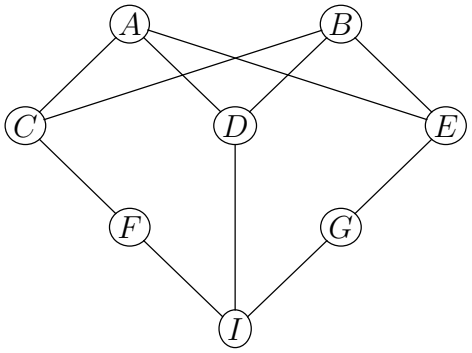


Figure 3: A subgraph of the graph G of Exercise 4 isomorphic to a subdivision of $K_{3,3}$.

(b) **No:** $32 - 2^5$, so $\log_2 32 = 5$.

(c) **Yes:** 2 is prime and 31 is not a power of 2, so $\log_2 32$ is irrational.

2. (a) **No:** the sequence $n/2^n$ vanishes, but all its terms are nonnegative, so it has an infinite descending chain.

   (b) **Yes:** this is a subset of the set $\mathbb{F}$ from Week 2, which is well ordered, so it is itself well ordered.

   (c) **No:** $\dfrac{n+2}{n+1} = 1 + \dfrac{1}{n+1}$ is the sum of a constant and a sequence that is an infinite descending chain, so it is also an infinite descending chain.

3. (a) **No:** this formula is *un*satisfiable, because the left-hand side is equivalent to **not**(P).

   (b) **No:** the premise of the main implication is equivalent to Q, so the proposition is equivalent to Q **implies** P, which isn't valid.

   (c) **Yes:** this is the modus ponens in disguise.

4. **True:** for example, we may choose as a domain the arithmetics of natural numbers, give type $\mathbb{N}$ to x and y, and interpret $P(x, y)$ as $x > y$. Then the formula takes the meaning "for every natural number there is a smaller natural number", which is false.

5. (a) **No:** from $(24, 24)$ we can move to $(30, 18)$.

   (b) **No:** from $(17, 0)$ we can move to $(0, 17)$.

   (c) **Yes:** $\gcd(30, 24) = 6$, so if b and ℓ are initially both multiples of a divisor of 6, they will remain so at every step.

6. (a) **Yes.**
   (b) **No:** she will have a suitor, but not necessarily the same.
   (c) **No:** the woman might reject him later, in which case he will erase her from her list in the evening.

7. (a) **No:** the base case $f(0)$ is missing.
   (b) **Yes:** as $g(0) = 1$, the value $n/g(n-1)$ is positive for every $n \geq 1$, and can be used as a denominator in a fraction.
   (c) **No:** for $n = 1$ the denominator is 0, so $h(1)$ is undefined.

8. (a) **No:** $43 \text{ XOR } 27 \text{ XOR } 48 = 0$, so this is a winning position for the *second* player.
   (b) **No:** $33 \text{ XOR } 17 \text{ XOR } 48 = 0$, so this is a winning position for the *second* player.
   (c) **Yes:** $43 \text{ XOR } 17 \text{ XOR } 38 = 28$, so this is a winning position for the first player.

9. **True:** this is the Schröder-Bernstein theorem. Remember that A surj B is equivalent to B inj A.

10. (a) **No:** we know from Exercise session 8 that if L was recognizable, then so would be No-halt.
    (b) **No:** we know from Exercise session 8 that if L was recognizable, then so would be No-halt.
    (c) **Yes:** the program P which, given in input the string s, compiles P_s, constructs $t = \texttt{01}s\texttt{10}$, and runs P_s on t, halts if and only $\texttt{01}s\texttt{10} \in \text{lang}(P_s)$.

11. (a) **No:** see below.
    (b) **No:** see below.
    (c) **Yes:** $\gcd(10000, 17) = \gcd(47, 17) = 1$, and both exponents are multiples of $\phi(17)$.

12. (a) **No:** the equality $f(m \cdot n) = f(m) \cdot f(n)$ needs only be satisfied when $\gcd(m, n) = 1$.
    (b) **Yes.**
    (c) **No:** this condition is equivalent to saying that $f(1)$ is either 1 or 0.

13. (a) **Yes:** knowing p and q such that $pq = n$, the multiplicative inverse of e modulo $\phi(n)$ can be calculated with the Pulverizer.

    (b) **No:** that's just the encryption of the private key with the public key.

    (c) **No:** we already know that n is not prime.

14. **False:** it is equal to the number of edges.

15. (a) **No:** for example, the DAG could be made of 96 isolated vertices.

    (b) **Yes:** by Dilworth's lemma with $n = 96$ and $\ell = 7$.

    (c) **No:** for example, the DAG could be made of a chain of size 17 and 79 isolated vertices.

16. (a) **True:** a linear order is a weak partial order where every two elements are comparable.

    (b) **No:** strict partial orders are irreflexive and weak partial orders are reflexive, so no strict partial order on a nonempty subset can be a weak partial order.

    (c) **No:** every strict partial order is the *positive* walk relation of a DAG.

17. (a) **No:** this is a *strict* partial order; in fact, xRy if and only if $x > y$.

    (b) **No:** this relation is not antisymmetric; for example, $\lceil 1/2 \rceil \leq \lceil 1 \rceil$ and $\lceil 1 \rceil \leq \lceil 1/2 \rceil$, but $1/2 \neq 1$.

    (c) **Yes:** in fact, xTy if and only if $x \leq y$.

18. (a) **No:** see below.

    (b) **Yes.**

    (c) **No:** see above.

19. **True:** a forest with 47 vertices and 3 connected components has only 50 edges.

20. (a) **Yes:** such a graph is a tree, and finite trees are planar.

    (b) **No:** a planar graph with 17 vertices can have at most $3 \cdot 17 - 6 = 45$ edges.

    (c) **No:** a bipartite planar graph with 17 vertices can have at most $2 \cdot 17 - 4 = 30$ edges.