Algoritmica Avanzata – CdL Magistrale in Ingegneria Informatica
Compito, 22/6/2015 (Durata: 2h30m)

Nome, Cognome, Matricola: _____

Prima parte: Domande Teoriche

Si risponda in modo **rigoroso, esauriente e conciso** alle tre domande di teoria elencate di seguito. Si ricorda che per accedere alla correzione della seconda parte, bisogna conseguire un punteggio complessivamente sufficiente alla prima parte.

T1 Dato un grafo completo, non orientato e con pesi nonnegativi, si dimostri che il costo di un albero di copertura di costo minimo è minore o uguale del costo di un tour di costo minimo.

Solution: Take the optimal tour $C^\star$ and remove an arbitrary edge e from the tour. Then, the remaining edges form a spanning tree T' of G, whose cost is clearly at least as much as the cost of a minimum spanning tree $T^\star$. But then

$$\text{cost}(T^\star) \leq \text{cost}(T') \leq \text{cost}(C^\star).$$

T2 Si dimostri che per $a > b \geq 1$, se l'esecuzione di EUCLID(a, b) effettua $k \geq 1$ chiamate (inclusa quella più esterna), allora $a \geq F_{k+2}$ e $b \geq F_{k+1}$.

Solution: By induction on k. For $k = 1$, the property holds since $b \geq 1 = F_2$ and $a \geq 2 = F_3$. For $k > 1$, let the property hold up to $k - 1$. We have that EUCLID(a, b) calls EUCLID$(b, a \bmod b)$, which must make exactly $k-1$ calls. By the inductive hypothesis, we then have $b \geq F_{(k-1)+2} = F_{k+1}$ and $a \bmod b \geq F_{(k-1)+1} = F_k$. Finally, by the division theorem, we have that $a = \lfloor a/b \rfloor b + (a \bmod b) \geq b + (a \bmod b) \geq F_{k+1} + F_k = F_{k+2}$.

T3 Si provi che se un multigrafo $\mathcal{G} = (V, \mathcal{E})$ ha un taglio minimo di cardinalità k, allora $|\mathcal{E}| \geq k|V|/2$.

Solution: Let $C^\star$ be a minimum cut. For each node $v \in V$, the set of its incident edges $N(v)$ is clearly a cut, disconnecting v from the other nodes in G. Therefore, $\forall v \in V : \deg(v) = |N(v)| \geq |C^\star| = k$. Finally, $2|\mathcal{E}| = \sum_{v \in V} \deg(v) \geq k|V|$ and the thesis follows.

Seconda Parte: Risoluzione di Problemi

Si forniscano soluzioni motivate e rigorose ai tre problemi seguenti.

Esercizio 1 [11 punti] Il problema MIN-EXACT-2-COVER ha come istanza generica una coppia $(X, \mathcal{F})$, formata da un insieme di elementi X e da una famiglia $\mathcal{F}$ di sottoinsiemi di X, con la seguente proprietà:

$$\forall x \in X : |\{F \in \mathcal{F} : x \in F\}| = 2.$$

In altre parole, ogni elemento di X compare **esattamente** in due sottoinsiemi di $\mathcal{F}$. Il problema richiede di determinare la sottofamiglia $\mathcal{C}^\star \subseteq \mathcal{F}$ di cardinalità minima per cui $X = \bigcup_{F \in \mathcal{C}^\star} F$. Si determini un algoritmo di 2-approssimazione per MIN-EXACT-2-COVER.

Answer: We can use the same approach used for VERTEX-COVER to build a cover $\mathcal{C}$. While there are uncovered elements $x \in X$, we pick an arbitrary one and put **both** subsets containing x in $\mathcal{C}$. The pseudocode follows.

APPROX-ME2C$(X, \mathcal{F})$
$\mathcal{C} \leftarrow \emptyset$; $S \leftarrow X$
while $S \neq \emptyset$ **do**
    $\star$ Select $x \in S$ arbitrarily $\star$
    $\mathcal{C} \leftarrow \mathcal{C} \cup \{F \in \mathcal{F} : x \in F\}$
    $S \leftarrow S - \bigcup_{x \in F} F$
return $\mathcal{C}$

The procedure clearly runs in polynomial time and correctly returns a cover. Let A denote the set of objects selected in the first line of the **while** loop. Since each objects is contained in two subsets, it follows that, on exit, $|\mathcal{C}| \leq 2|A|$, thus $|\mathcal{C}|/2 \leq |A|$. Moreover, observe that no two objects in A can belong to the same subset (or otherwise, during the iteration at which the first is selected, the second would be removed from S and thus could never be selected in subsequent iterations). Therefore, there must be at least one subset for each object in A in the optimal solution $\mathcal{C}^\star$. Putting it all together we conclude that

$$|\mathcal{C}|/2 \leq |A| \leq |\mathcal{C}^\star| \text{ whence } \rho = \frac{|\mathcal{C}|}{|\mathcal{C}^\star|} \leq 2.$$

As an aside, observe that MIN-EXACT-2-COVER is just a different formulation of VERTEX-COVER for multigraphs. Indeed, given $(X, \mathcal{F})$, let $\mathcal{F} =$

$\{F_1, F_2, \ldots, F_n\}$, define the multigraph $\mathcal{G} = (V, \mathcal{E})$ where $V = \{v_1, v_2, \ldots, v_n\}$ and $\{v_i, v_j\} \in \mathcal{E} \leftrightarrow m_{ij} = |F_i \cap F_j| > 0$. The edge's multiplicity is m_{ij}. Clearly, every instance $(X, \mathcal{F})$ corresponds to one multigraph $\mathcal{G} = (V, \mathcal{E})$, and every multigraph $\mathcal{G} = (V, \mathcal{E})$ induces a single instance $(X, \mathcal{F})$. Under this correspondence, determining the minimum covering subfamily $\mathcal{C}^\star \subseteq \mathcal{F}$ corresponds to determining the minimum vertex cover of $\mathcal{G}$, which in turn can be determined using the known approximation algorithm applied to G, ignoring the multiplicities.

□

Esercizio 2 [10 punti] Si determini 25^{-1} mod 84 giustificando il procedimento adottato.

Answer: Since it must be $\gcd(84, 25) = 1$, we call EXTENDED_EUCLID$(84, 25)$ (from now on, we use the shorthand EE for EXTENDED_EUCLID) to return $(1, (x, y))$, where $1 = 84 \cdot x + 25 \cdot y$, whence $y \equiv 25^{-1}$ mod 84. Recall that in the conquer phase of EE, if $\{1, (\bar{x}, \bar{y})\}$ is the structure returned by EE$(b, a \bmod b)$, then the outer call EE(a, b) will return $\{1, (\bar{y}, \bar{x} - \lfloor a/b \rfloor \bar{y})\}$. We have the following series of calls:

$$\text{EE}(84, 25) \to \text{EE}(25, 9) \to \text{EE}(9, 7) \to \text{EE}(7, 2) \to \text{EE}(2, 1) \to \text{EE}(1, 0),$$

returning the following structures (in reverse order):

$$\{1, (1, 0)\} \to \{1, (0, 1)\} \to \{1, (1, -3)\} \to \{1, (-3, 4)\} \to \{1, (4, -11)\} \to \{1, (-11, 37)\}.$$

Therefore, $1 = 84 \cdot (-11) + 25 \cdot 37$, whence $25^{-1} \bmod 84 = 37$.

□

Esercizio 3 [11 punti] Siano $X_1, X_2, \ldots, X_n$ variabili di Bernoulli indipendenti, con $\Pr(X_i = 1) = p_i$, $1 \leq i \leq n$. Sia $X = \sum_{i=1}^{n} X_i$ e $\mu = E[X]$. Si dimostri che per $R \geq 6\mu$ si ha:

$$\Pr(X \geq R) < 2^{-R}.$$

(*Suggerimento:* Si ponga $R = (1 + \delta)\mu$ e si presti attenzione al fatto che $\delta > 1$)

Answer: Following the hint, we let $R = (1 + \delta)\mu$, where $1 + \delta \geq 6$ (whence $\delta \geq 5 > 1$). We apply the Chernoff bound as follows:

$$\begin{aligned} \Pr(X \geq R) &= \Pr(X \geq (1 + \delta)\mu) \\ &\leq \left(\frac{e^\delta}{(1 + \delta)^{1+\delta}} \right)^\mu \end{aligned}$$

$$
\begin{aligned}
&\leq \left(\frac{e^{1+\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu} \\
&= \left(\frac{e}{(1+\delta)}\right)^{(1+\delta)\mu} \\
&\leq (e/6)^{R} \\
&< 2^{-R}.
\end{aligned}
$$

□

Algoritmica Avanzata – CdL Magistrale in Ingegneria Informatica
Compito, 8/7/2015 (Durata: 2h30m)

Nome, Cognome, Matricola: _____

Prima parte: Domande Teoriche

Si risponda in modo **rigoroso, esauriente e conciso** alle tre domande di teoria elencate di seguito. Si ricorda che per accedere alla correzione della seconda parte, bisogna conseguire un punteggio complessivamente sufficiente alla prima parte.

T1 Dato un grafo non orientato $G = (V, E)$, si dimostri che la cardinalità di un generico vertex cover è sempre maggiore della cardinalità di un generico matching.

Solution: The edges of any matching M do not share endpoints, therefore, at least one endpoint per edge is needed for that edge to be covered by any vertex cover V'. Therefore $|M| \leq |V'|$.

T2 Si enunci e si provi la proprietà di sottostruttura alla base dell'algoritmo EUCLID(a, b) per $a \geq b > 0$.

Solution: The substructure property claims that for $a \geq b > 0$, $g = \gcd(a, b) = \gcd(b, a \bmod b) = g'$. The proof is as follows. By the division theorem, $\exists q \in \boldsymbol{Z} : a = qb + a \bmod b$, whence $a \bmod b = a - qb$. By Bezout's identity we also know that $\exists x, y \in \boldsymbol{Z} : g' = bx + (a \bmod b)y = bx + (a - qb)y = ay + b(x - qy)$. Then, g' is a positive integer linear combination of a and b, hence $g' \geq g$. Also, $(g'|b) \wedge (g'|a \bmod b) \Rightarrow g'|(qb + a \bmod b) = a$. Therefore g' is a common divisor of a and b , hence $g' \leq g$.

T3 Si fornisca una stima asintotica stretta al numero medio di estrazioni con reimbussolamento dall'urna $U_n = \{1, 2, \ldots, n\}$ necessarie a ottenere tutti i valori presenti nell'urna (*coupon collecting*).

Solution: Let Z be the number of needed extractions. Then, $Z = \sum_{i=1}^{n} Z_i$, where Z_i is a geometric variable denoting the number of extractions needed to see a new value after $i-1$ distinct values have already been obtained. We have that $E[Z_i] = 1/p_i$, with $p_i = (n - i + 1)/n$. By linearity of expectation we have:

$$E[Z] = \sum_{i=1}^{n} \frac{1}{p_i} = n \sum_{i=1}^{n} \frac{1}{n - i + 1} = n \sum_{k=1}^{n} \frac{1}{k} = nH(n) = \Theta(n \log n).$$

Seconda Parte: Risoluzione di Problemi

Si forniscano soluzioni motivate e rigorose ai tre problemi seguenti.

Esercizio 1 [11 punti] Nel problema del BIN-PACKING, dati n oggetti $o_1, o_2, \ldots, o_n$ associati ai pesi positivi $w_1, w_2, \ldots, w_n$ e una capacità $W \geq \max\{w_i : 1 \leq i \leq n\}$ si devono disporre gli n oggetti nel minimo numero $k^\star$ di scatole $S_1, S_2, \ldots, S_{k^\star}$ in modo tale che $\sum_{o_i \in S_j} w_i \leq W$, per $1 \leq j \leq k^\star$. Ad esempio, per la istanza $\langle w_1 = 1, w_2 = 4, w_3 = 3, W = 4\rangle$ la soluzione ottima è $k^\star = 2$, ottenuta con $S_1 = \{o_1, o_3\}$ e $S_2 = \{o_2\}$. Si dimostri che il semplice algoritmo greedy che sistema gli oggetti in scatole uno per volta, da o_1 a o_n, creando, all'iterazione i, una nuova scatola se nessuna delle scatole create precedentemente può accomodare anche l'oggetto o_i, è un algoritmo di 2-approssimazione per il problema.
(*Suggerimento:* si dimostri che al termine dell'algoritmo ci può essere al più **una** singola scatola contenente oggetti di peso complessivo $< W/2$ e si usi questo fatto per limitare superiormente il numero di scatole ritornate dall'algoritmo in funzione del peso complessivo degli n oggetti.)

Answer: We proceed to prove the hint: assume for the sake of contradiction that by the end of the algorithm there are two boxes containing objects of total weight $< W/2$. Consider the iteration i at which the second such box is created. But then obect o_i with $w_i < W/2$ is placed in the box, which contradicts the greedy rule, since the first box of weight $< W/2$ could have accommodated o_i without the need of creating a new box. Let k_G be the number of boxes created by the algorithm. The previous property implies that $\sum_{i=1}^{n} w_i > (k_G - 1)W/2$. Also, let $k^\star$ be the optimal solution. Clearly, it must be $k^\star \geq \left(\sum_{i=1}^{n} w_i\right)/W$. Therefore:

$$(k_G - 1) < 2\sum_{i=1}^{n} w_i/W \leq 2k^\star \Rightarrow k_G \leq 2k^\star \Rightarrow \rho = k_G/k^\star \leq 2.$$

□

Esercizio 2 [10 punti] Dato $n = 11 \times 23 = 253$ e la chiave pubblica $P_A = (7, 253)$, si determini la corrispondente chiave segreta S_A e la relativa funzione di decodifica $S_A(M)$ ad essa associata nel criptosistema a chiave pubblica RSA.

Answer: We have that $\phi(n) = (11 - 1) \cdot (23 - 1) = 220$. Given the public key $P = (7, 253)$, in order to obtain the corresponding secret key, we must determine the multiplicative inverse of 7 in $\boldsymbol{Z}^\star_{220}$. In turn, such an inverse can be

obtained by applying Algorithm EXTENDED EUCLID (EE) to determine Bezout relation between 1=gcd(220, 7), 220 and 7. On (220, 7), EE performs calls on (7, 3), (3, 1), and finally (1, 0). From bottom up, the values returned by these calls are $(1, \{1, 0\})$, $(1, \{0, 1\})$, $(1, \{1, -2\})$ and finally $(1, \{-2, 63\})$. It follows that $S = (63, 253)$, hence, for any message $M \in \boldsymbol{Z}_{253}$, $S(M) = M^{63} \bmod 253$. □

Esercizio 3 [11 punti] Si supponga di effettuare $n \geq e^3$ lanci di una moneta bilanciata ($\Pr(\text{testa}) = \Pr(\text{coda}) = 1/2$), e sia X il numero di teste ottenute. Utilizzando i lemmi di Chernoff si determini il più piccolo valore di t per cui si possa provare che

$$\Pr(X > t) \leq \frac{1}{n}.$$

(*Suggerimento:* Si ponga $t = (1 + \delta)E[X]$, supponendo $\delta < 1 \ldots$)

Answer: Following the hint, let $t = (1+\delta)E[X] = (1+\delta)n/2$, and assume $\delta < 1$. We then have

$$\Pr(X > t) = \Pr(X > (1 + \delta)E[X]) < e^{-\delta^2 E[x]/3} = e^{-\delta^2 n/6}.$$

It then suffices to make sure that $\delta^2 n/6 = \ln n$, so that $e^{-\delta^2 n/6} = e^{-\ln n} = 1/n$. Therefore $\delta = \sqrt{6(\ln n)/n}$ (< 1 for $n > e^3$), which implies $t = n/2 + \sqrt{3n(\ln n)/2}$.

□

Algoritmica Avanzata – CdL Magistrale in Ingegneria Informatica
Compito, 8/7/2015 (Durata: 2h30m)

Nome, Cognome, Matricola: _____

Prima parte: Domande Teoriche

Si risponda in modo **rigoroso, esauriente e conciso** alle tre domande di teoria elencate di seguito. Si ricorda che per accedere alla correzione della seconda parte, bisogna conseguire un punteggio complessivamente sufficiente alla prima parte.

T1 Dato un grafo non orientato $G = (V, E)$, si dimostri che la cardinalità di un generico vertex cover è sempre maggiore della cardinalità di un generico matching.

Solution: The edges of any matching M do not share endpoints, therefore, at least one endpoint per edge is needed for them to be covered by any vertex cover V'. Therefore $|M| \leq |V'|$.

T2 Si enunci e si provi la proprietà di sottostruttura alla base dell'algoritmo EUCLID(a, b) per $a \geq b > 0$.

Solution: The substructure property for $a \geq b > 0$ claims that $g = \gcd(a, b) = \gcd(b, a \bmod b) = g'$. By the division theorem, $\exists q \in \boldsymbol{Z}^+ : a = qb + a \bmod b$, whence $a \bmod b = a - qb$. By Bezout's identity we also know that $\exists x, y \in \boldsymbol{Z} : g' = bx + (a \bmod b)y = bx + (a - qb)y = ay + b(x - qy)$. Since g' is a positive integer linear combination of a and b, it must be $g' \geq g$. Also, $(g'|b) \wedge (g'|a \bmod b) \Rightarrow g'|(qb + a \bmod b) = a$. Therefore g' is a common divisor of a and b whence $g' \leq g$.

T3 Si fornisca una stima asintotica stretta al numero medio di estrazioni con reimbussolamento dall'urna $U_n = \{1, 2, \ldots, n\}$ necessarie a ottenere tutti i valori presenti nell'urna (*coupon collecting*).

Solution: Let Z be the number of needed extractions. Then, $Z = \sum_{i=1}^{n} Z_i$, where Z_i is a geometric variable denoting the number of extractions needed to see a new number after $i - 1$ distinct numbers have already been obtained. We have that $E[Z_i] = 1/p_i$, with $p_i = (n - i + 1)/n$. By linearity of expectation we have:

$$E[Z] = \sum_{i=1}^{n} \frac{1}{p_i} = n \sum_{i=1}^{n} \frac{1}{n - i + 1} = n \sum_{k=1}^{n} \frac{1}{k} = nH(n) = \Theta(n \log n).$$

Seconda Parte: Risoluzione di Problemi

Si forniscano soluzioni motivate e rigorose ai tre problemi seguenti.

Esercizio 1 [11 punti] Il problema PARTITION ha come istanza $\langle S \rangle$, dove S è un insieme finito di naturali positivi e $T = \sum_{s \in S} s$ è un numero dispari. Il problema richiede di determinare il sottoinsieme $S^\star \subseteq S$ che minimizza la quantità

$$\left| \sum_{s \in S - S^\star} s - \sum_{s \in S^\star} s \right|.$$

Punto 1 [redacted] Si dimostri: $(S^\star = OPT(\langle S \rangle)) \Rightarrow (S - S^\star = OPT(\langle S \rangle))$.

Punto 2 [redacted] Usando il Punto 1, di dimostri che esiste una soluzione $S^\star$ ottima per PARTITION, con $\sum_{s \in S^\star} s \leq (T-1)/2$. Si dimostri inoltre che tale soluzione $S^\star$ è ottima anche per l'istanza $\langle S, (T-1)/2 \rangle$ di SUBSET-SUM.

[redacted]

Answer:

Point 1 Let $S^\star = OPT(\langle S \rangle)$. The sum function associated to $S - S^\star$ is

$$\begin{aligned} cost(S - S^\star) &= \left| \sum_{s \in S - (S - S^\star)} s - \sum_{s \in (S - S^\star)} s \right| \\ &= \left| \sum_{s \in S^\star} s - \sum_{s \in (S - S^\star)} s \right| \\ &= \left| \sum_{s \in S - S^\star} s - \sum_{s \in S^\star} s \right| \\ &= cost(S^\star), \end{aligned}$$

and the thesis follows.

Point 2 By Point 1, given an optimal solution S', we know that $S - S'$ is also optimal. Moreover, we clearly have have that $\sum_{s \in S'} s + \sum_{s \in S - S'} s = \sum_{s \in S} s = T$. Therefore it must be either $\sum_{s \in S'} s \leq \lfloor T/2 \rfloor = (T-1)/2$ or $\sum_{s \in S - S'} s \leq (T-1)/2$. It then suffices to choose $S^\star$ as the (optimal) solution of minimum sum between S' and $S - S'$. Observe that if $S^\star$ where not optimal for instance $\langle S, (T-1)/2 \rangle$

of SUBSET-SUM, there would be a subset $\bar{S}$ with $\sum_{s\in S^\star} s < \sum_{s\in \bar{S}} s \leq (T-1)/2$ (and therefore $\sum_{s\in S-\bar{S}} s < \sum_{s\in S-S^\star} s$), but then

$$0 < \sum_{s\in S-\bar{S}} s - \sum_{s\in \bar{S}} s < \sum_{s\in S-S^\star} s - \sum_{s\in S^\star} s,$$

which contradicts that $S^\star = OPT(\langle S\rangle)$.

[redacted]

Svolgimento errato. Ignorare.

[redacted]

□

Esercizio 2 [10 punti] Dato $n = 11 \times 23 = 253$ e la chiave pubblica $P_A = (7, 253)$, si determini la corrispondente chiave segreta S_A e la relativa funzione di decodifica $S_A(M)$ ad essa associata nel criptosistema a chiave pubblica RSA.

Answer: We have that $\phi(n) = (11-1)\cdot(23-1) = 220$. Given the public key $P = (7, 253)$, in order to obtain the corresponding secret key, we must determine the multiplicative inverse of 7 in $\boldsymbol{Z}^\star_{220}$. In turn, such an inverse can be obtained by applying Algorithm EXTENDED EUCLID (EE) to determine Bezout relation between 1=gcd(220, 7), 220 and 7. On (220, 7), EE performs calls on (7, 3), (3, 1), and finally (1, 0). From bottom up, the values returned by these calls are $(1, \{1, 0\})$, $(1, \{0, 1\})$, $(1, \{1, -2\})$ and finally $(1, \{-2, 63\})$. It follows that $S = (63, 253)$, hence, for any message $M \in \boldsymbol{Z}_{253}$, $S(M) = M^{63} \bmod 253$. □

Esercizio 3 [11 punti] Si supponga di effettuare $n \geq e^3$ lanci di una moneta bilanciata (Pr(testa) = Pr(coda) = 1/2), e sia X il numero di teste ottenute. Utilizzando i lemmi di Chernoff si determini il più piccolo valore di t per cui si possa provare che

$$\Pr(X > t) \leq \frac{1}{n}.$$

(*Suggerimento:* Si ponga $t = (1 + \delta)E[X]$, supponendo $\delta < 1 \ldots$)

Answer: Following the hint, let $t = (1+\delta)E[X] = (1+\delta)n/2$, and assume $\delta < 1$. We then have

$$\Pr(X > t) = \Pr(X > (1 + \delta)E[X]) < e^{-\delta^2 E[x]/3} = e^{-\delta^2 n/6}.$$

It then suffices to make sure that $\delta^2 n/6 = \ln n$, so that $e^{-\delta^2 n/6} = e^{-\ln n} = 1/n$. Therefore $\delta = \sqrt{6(\ln n)/n}$ (< 1 for $n > e^3$), which implies $t = n/2 + \sqrt{3n(\ln n)/2}$.

□

Algoritmica Avanzata – CdL Magistrale in Ingegneria Informatica
Compito, 24/2/2016 (Durata: 2h)

Nome, Cognome, Matricola: _____

Seconda Parte: Risoluzione di Problemi

Si forniscano soluzioni motivate e rigorose ai tre problemi seguenti.

Esercizio 1 [11 punti] Un grafo **orientato** è fortemente connesso se in esso esite un cammino tra una qualsiasi coppia ordinata di nodi. Dato un tale grafo $G = (V, E)$ con pesi sugli archi $w : E \to \boldsymbol{Z}^+$, il suo **diametro** Δ_G è il **massimo** peso di un cammino **minimo** tra una coppia ordinata di nodi. In altre parole, se π^*_{uv} denota un camminimo minimo da u a v e $w(\pi^*_{uv})$ la sua lunghezza, allora

$$\Delta_G = \max_{(u,v)\in V\times V} \{w(\pi^*_{uv})\}\,.$$

(Si noti che in generale $w(\pi^*_{uv}) \neq w(\pi^*_{vu})$.) Si noti che il calcolo basato sulla definizione di Δ_G richiede richiede di calcolare il peso di n^2 cammini minimi.

Punto 1 [8 pt] Si provi che la quantità $\max_{v\in V}\{w(\pi^*_{vs}), w(\pi^*_{sv})\}$, dove $s \in V$ è un nodo arbitario, costituisce una 2-approssimazione per Δ_G, ovvero che

$$1 \leq \frac{\Delta_G}{\max_{v\in V}\{w(\pi^*_{vs}), w(\pi^*_{sv})\}} \leq 2.$$

Punto 2 [3 pt] Usando il Punto 1, si discuta (a parole) un algoritmo efficiente per il calcolo approssimato del diametro di un grafo orientato.

Answer:

Point 1 First, we clearly have that $\Delta_G \geq \max_{v\in V}\{w(\pi^*_{vs}), w(\pi^*_{sv})\}$, since Δ_G is the maximum of the larger set containing all possible weights of shortest paths, rather than only those starting or ending at s. Thus, the lower bound on the ratio follows. Let now u' and v' be two nodes at the endpoints of a shortest path of weight Δ_G, that is

$$\Delta_G = \max_{(u,v)\in V\times V} \{w(\pi^*_{uv})\} = w(\pi^\star_{u'v'}).$$

We have that the (not necessarily simple) path $\langle \pi^\star_{u's}, \pi^\star_{sv'} \rangle$ connects u' and v' and has weight $w(\pi^\star_{u's}) + w(\pi^\star_{sv'}) \leq 2\max_{v\in V}\{w(\pi^\star_{vs}), w(\pi^\star_{sv})\}$, whence it must be

$\Delta_G \leq 2 \max_{v \in V}\{w(\pi^\star_{vs}) + w(\pi^\star_{sv})\}$, since Δ_G is the weight of the shortest path between u' and v'. The upper bound on the ratio follows.

Point 2 We can pick an arbitrary node $s \in V$ and run Dijkstra's algorithm on G to find the weights of the shortest paths from s to all nodes in V. We can also find the the weights of the shortest paths from all nodes in V to s by reversing all edges and again applying Dijkstra to the reverse graph using s as root. We could then return the largest weight computed, a 2-approximation to Δ_G according to Point 1. Observe that this method requires time $O(|E| + |V| \log |V|)$, which on sparse graphs can be substantially better than the $\Omega(|V|^2)$ time needed to compute all possibile shortest path weights.

□

Esercizio 2 [10 punti] Si consideri un criptosistema a chiave pubblica di tipo RSA in cui il dominio dei messaggi è $\boldsymbol{Z}_n$, con $n = 11 \times 23 = 253$. Data la chiave pubblica $P = (7, 253)$ determinare la corrispondente chiave segreta S e la relativa funzione di decodifica $S(M)$ ad essa associata.

Answer: We have that $\phi(n) = (11 - 1) \cdot (23 - 1) = 220$. Given the public key $P = (7, 253)$, in order to obtain the corresponding secret key, we must determine the multiplicative inverse of 7 in $\boldsymbol{Z}^\star_{220}$. In turn, such an inverse can be obtained by applying Algorithm EXTENDED EUCLID (EE) to determine the Bezout equality between 1=gcd(220, 7), 220 and 7. On (220, 7), EE performs calls on (7, 3), (3, 1), and finally (1, 0). From bottom up, the values returned by these calls are $(1, \{1, 0\})$, $(1, \{0, 1\})$, $(1, \{1, -2\})$ and finally $(1, \{-2, 63\})$. It follows that $S = (63, 253)$, hence, for any message $M \in \boldsymbol{Z}_{253}$, $S(M) = M^{63} \bmod 253$. □

Esercizio 3 [11 punti] Il problema MAX-3-CNF-SPARSESAT richiede di determinare, data una formula $\langle \Phi(x_1, \ldots, x_n) = C_1 \wedge \ldots \wedge C_m \rangle$ in formato 3-CNF, il massimo numero di clausole che contengano **un solo** letterale vero sotto un dato assegnamento di verità. Si fornisca un semplice algoritmo di approssimazione randomizzato $A(\langle \Phi \rangle)$ per MAX-3-CNF-SPARSESAT e se ne studi il fattore di approssimazione $OPT/E[A(\langle \Phi \rangle)]$.

Answer: We propose the following simple randomized algorithm:

$A(\langle \Phi(\boldsymbol{x}) \rangle)$
$n \leftarrow \boldsymbol{x}.len$
$\star$ Let $\Phi(\boldsymbol{x}) = \bigwedge_{i=1}^{m} C_i$ $\star$
for $j \leftarrow 1$ **to** n **do** $b_j \leftarrow \text{RANDOM}(\{0, 1\})$
$count \leftarrow 0$
for $i \leftarrow 1$ **to** m **do**
    if ($\star C_i(\boldsymbol{b})$ features only one true literal $\star$)
        then $count \leftarrow count + 1$
return $count$

Let $X_i = 1$ if the i-th clause C_i contains only one true literal under the random assignment $\boldsymbol{b}$. Then

$$E[A(\langle \Phi \rangle)] = E[count] = E[\sum_{i=1}^{m} X_i] = \sum_{i=1}^{m} E[X_i] = \sum_{i=1}^{m} \Pr(X_i = 1).$$

Since there are 3 over the 8 configurations of the three distinct variables associated to the literals of C_i that feature only one true literal, we have $\Pr(X_i = 1) = 3/8$ for $1 \leq i \leq m$, whence $E[A(\langle \Phi \rangle)] = 3m/8$. It follows that

$$\rho_A = OPT/E[A(\langle \Phi \rangle)] \leq m/(3m/8) = 8/3.$$

□