

UVOD V RAČUNALNIŠTVO

Izpit

16.2.2015

1 Teoretična vprašanja

Na vprašanja odgovarjajte tako, da obkrožite črko pred odgovorom. Pri vsakem vprašanju je pravilen natanko en (1) odgovor. Vsak pravilen odgovor je vreden 3 točke, neodgovorjeno vprašanje 0 točk ter napačen odgovor -3 točke.

1. Namen IP (Internet Protocol) številke je:
 - (a) Sporočanje namembnosti strežnika s to številko ostalim računalnikom v omrežju.
 - (b) Identifikacija računalnikov v internetnem omrežju.
 - (c) Identifikacija protokola po katerem bo potekala internetna komunikacija s tem strežnikom.
 - (d) Posredovanje javnega ključa strežnika s to številko.
2. TLS/SSL (Transport Layer Security/Secure Sockets Layer) protokol za varen prenos podatkov tipično uporablja:
 - (a) CRC kodo.
 - (b) DES šifriranje.
 - (c) RSA šifriranje.
 - (d) DES in RSA šifriranje.
3. Sortirni algoritem A ima povprečno časovno zahtevnost $O(0,5 \cdot n^2)$, sortirni algoritem B pa $O(2 \cdot n \cdot \log_2 n)$. Kateri algoritem se nam bolj splača uporabiti za sortiranje 16 števil?
 - (a) Algoritem A.
 - (b) Algoritem B.
 - (c) Oba sta enako dobra.
 - (d) Imamo premalo informacij, da bi lahko to napovedali.
4. Z vidika izračunljivosti uredi naslednje programske paradigme (simbol $>$ pomeni »lahko izračuna več« oz. »reši več problemov«):
 - (a) Imperativna $>$ logična $>$ funkcijska.
 - (b) Funkcijska $>$ logična $>$ imperativna.
 - (c) Imperativna $>$ funkcijska $>$ logična.
 - (d) Vse tri so enakovredne.
5. »Programa, ki bi za poljuben drug program in za poljuben vhod povedal ali bo le-ta vrnil točno določen (npr. pravilen) rezultat, ni mogoče napisati.«
 - (a) Trditev je resnična.
 - (b) Trditev ni resnična.
 - (c) Trditev je resnična, a le za logično programsko paradigmo.
 - (d) Nimamo zadosti informacij, da bi lahko ocenili resničnost trditve.

6. Gramatika, ki vsebuje samo naslednje BNF pravilo: $\langle \text{bnum} \rangle ::= 0 \mid 1 \mid \langle \text{bnum} \rangle \langle \text{bnum} \rangle \mid \Lambda$
- Ne generira vseh binarnih števil.
 - Je dvoumna.
 - Ni dvoumna, a ne generira vseh binarnih števil.
 - Ni dvoumna in generira vsa binarna števila.
7. S pomočjo samo vrat NOR (not OR):
- Ni možno zgraditi vrat OR.
 - Je možno zgraditi računalnik, ki je Turing-popoln.
 - Ni možno zgraditi računalnika, ki je Turing-popoln.
 - Drži (a) in (c).
8. Kontrolne operacije kot so npr. *if*, *else* in *while*:
- Niso sestavni del vsakega programskega jezika.
 - So sestavni del le psevdokode in skriptnih jezikov (kot npr. Python).
 - Drži (a) in (b).
 - Nič od naštetega.
9. S pomočjo paritetnega bita (ki ni dodan spodnjim podatkom) lahko zaznamo napako pri prenosu:
- $1111 \rightarrow 0000$
 - $1011 \rightarrow 0000$
 - $1001 \rightarrow 0000$
 - Pri (a) in (c).
 - Pri (a) in (b) in (c).
10. Algoritem vsote produktov (angl. *Sum-of-Products*) za izgradnjo vezij:
- Vedno zgradi optimalno vezje glede na število vrat (čim manjše).
 - Skoraj vedno (a ne vedno) zgradi optimalno vezje glede na število vrat.
 - Ne uporablja vrat NOT, ampak samo vrata AND in OR.
 - Nič od naštetega.

Binary Op Code	Operation	Meaning
0000	LOAD X	$\text{CON}(X) \rightarrow R$
0001	STORE X	$R \rightarrow \text{CON}(X)$
0010	CLEAR X	$0 \rightarrow \text{CON}(X)$
0011	ADD X	$R + \text{CON}(X) \rightarrow R$
0100	INCREMENT X	$\text{CON}(X) + 1 \rightarrow \text{CON}(X)$
0101	SUBTRACT X	$R - \text{CON}(X) \rightarrow R$
0110	DECREMENT X	$\text{CON}(X) - 1 \rightarrow \text{CON}(X)$
0111	COMPARE X	if $\text{CON}(X) > R$ then $\text{GT} = 1$ else 0 if $\text{CON}(X) = R$ then $\text{EQ} = 1$ else 0 if $\text{CON}(X) < R$ then $\text{LT} = 1$ else 0
1000	JUMP X	Get the next instruction from memory location X.
1001	JUMPGT X	Get the next instruction from memory location X if $\text{GT} = 1$.
1010	JUMPEQ X	Get the next instruction from memory location X if $\text{EQ} = 1$.
1011	JUMPLT X	Get the next instruction from memory location X if $\text{LT} = 1$.
1100	JUMPNEQ X	Get the next instruction from memory location X if $\text{EQ} = 0$.
1101	IN X	Input an integer value from the standard input device and store into memory cell X.
1110	OUT X	Output, in decimal notation, the value stored in memory cell X.
1111	HALT	Stop program execution.

2 Praktične naloge

1. Imamo glavni pomnilnik velikosti 16 GB in dostopnim časom 24 ns.

- Kako velik je naslovni register? [5 točk]

- Povprečni dostopni čas želimo z uporabo predpomnilnika zmanjšati na 18 ns. Kakšen dostopni čas mora imeti predpomnilnik, če vemo, da je verjetnost zadetka enaka 75%? [10 točk]

2. Napišite program v zbirnem jeziku, ki s standardnega vhoda bere števila, dokler ne vpišemo nič in na koncu izpiše vsoto vseh vpisanih negativnih števil. [20 točk]

3. Napišite BNF gramatiko, ki sprejme palindrom. Palindrom je niz, ki se z leve bere enako kot z desne, presledki pa se ne upoštevajo (primer: *celsimislec*). Tudi ena sama črka ali prazna beseda Λ je palindrom. [20 točk]

4. Cezar se želi skrivoma sestati z Markom Antonijem – bodisi pri reki Tiberi ali v Areni – zato mu pošlje naslednje šifrirano sporočilo v angleščini (uporabil je angleško abecedo): "EVIRE". Mark Antonij ne pozna ključa, zato se loti dešifriranja. Kam naj gre na sestanek s Cezarjem? [15 točk]