教育部 112 年公費留學考試試題 103

科目：計算機結構 (全二頁，第一頁)

※可使用工程計算機(限僅具備＋、－、×、÷、% 、√、MR、MC、M+、M-、三角函數、對數、指數運算功能)

※以中文或英文作答均可，評分基準相同。

1. Short answer: (20 points 5 pts each)
   (a) What are the cycle time and clock rate?
   (b) If the current PC of a beq instruction is 0x80000, give the maximal byte address range that the instruction can branch to (with a 8-bit immediate field).
   (c) Execution time = CPU time + mem time. Given the fraction of the CPU time is 40%. $f_{cpu} = 40\,\%,\quad S_{cpu} = 2,\quad S_{mem} = 1.2 \to \infty$ What is the maximal and minimal speedup?
   (d) What is pipelining? Why does it improve CPU performance?

2. Assume that we will build a basic new CPU for NTCA (New Taiwan Computing Array):(35 points)

- In following questions, please explain the answer and **also fill each factor in the table**.
- Assume *N* instructions are executed by a NTCA processor and are broken down as instructions.

  R-type: 40%, *beq*: 30%, *lw*: 20% and *sw*: 10%.
- Assume the latencies for each stage of single-cycle NTCA1 are listed.

I-mem	ID	EX	D-MEM	WB
200ps	150ps	200ps	200ps	100ps

prog time = inst # × CPI × cycle_time

(a) (6 points) Give answers for the basic single-cycle NTCA1 on right.

(b) (9 points) Now we build a 5-stage pipelined NTCA2. Give answers for (b) NTCA2. What is the ideal speedup achieved by pipelining NTCA2 versus single-cycle NTCA1?

	Inst #	CPI	cycle time
(a) NTCA1			
(b) NTCA2			
(c) NTCA3			

(接下頁)

(c) (12 points) Now you would like to cut cost by giving a simpler NTCA3, which allows only register addressing for memory (no more immediate add). How many stages can the simple NTCA3 become? Will it be faster than NTCA2? Explain why and give answers for (c).

Original lw rd, rs1, immediate ;; rd = memory[rs1 + immediate]

replaced by

→ { addi rd, rs1, immediate ;; rd = rs1 + immediate
  { lw rd, rs1 ;; rd = memory[rs1]

(d) (8 points) Are there any impacts or changes due to NTCA3 on data forwarding or hazard stall detection? Explain why.

3. Memory hierarchy. (25 points)

(a) (6 points) Explain how a memory hierarchy with L1, L2, and main memory work.

(b) (6 points) Spatial locality and temporal locality are two key properties to maintain memory hierarchy. Give a short C code and specify statements that can illustrate these two locality types.

(c) (6 points) What is page table? How large is the page table of a 16GB system with 4KB/page? Why is a TLB needed for virtual memory?

(d) (7 points) Compare the key differences between cache memory and virtual memory.

4. Consider CPU, DMA(direct memory access) and I/O. (20 points)

(a) (6 points) Explain how DMA works with CPU for I/O operations.

(b) (6 points) If a machine cannot handle interrupt, the system will not be able to perform I/O via DMA. Argue the above statement correct or not?

(c) (8 points) How does CPU perform I/O tasks via memory-mapped I/O and I/O commands? Can we have DMA working with memory-mapped I/O?

教育部 112 年公費留學考試試題 104

科目：演算法 （全一頁）

※可使用工程計算機(限僅具備＋、－、×、÷、% 、√、MR、MC、M+、M-、三角函數、對數、指數運算功能)

※以中文或英文作答均可，評分基準相同。

1. Answer the following two questions

   (a) (10 points) Is it true that if $f(n) = O(g(n))$, $f(n) \geq 2$ and $g(n) \geq 2$, then $\log f(n) = O(\log g(n))$? Prove your answer.

   (b) (10 points) Is it true that if $f(n) = O(g(n))$, then $2^{f(n)} = O(2^{g(n)})$? Prove your answer.

2. You are running a restaurant with n seats. One day, many customers arrive. They form groups of different sizes. For each group of customers, you must either seat the whole group or they will leave. There are at least $\frac{n}{2}$ customers in total and all group sizes are less than n. Your goal is to serve as many customers as possible.

   (a) (20 points) Design an $O(n \log n)$-time 2-approximation algorithm. Briefly justify the correctness and analyze the running time.

   (b) (20 points) Design an $O(n^2)$-time algorithm which finds the optimal solution. Briefly justify the correctness and analyze the running time.

3. (20 points) Given a graph $G = (V, E)$ and a starting vertex $s \in V$, design an $O(V + E)$ algorithm that marks all vertices reachable from s using a path (not necessarily a simple path) with an even number of edges. Briefly justify the correctness and analyze the running time.

4. (20 points) A trader wants to travel to different cities and make trades. There are n cities $C_1, C_2, \ldots, C_n$. The trip must start and end at C_1. Every time the trader reaches a new city C_i, he can trade there and earn r_i dollars. (He does not get any revenue by passing through C_i the second time.) On the other hand, traveling from city C_i to city C_j costs f_{ij} every time. He wants to decide whether there exists a trip with net revenue at least some given constant k or not. (Net revenue is the total revenue from trading minus the total cost of traveling.) This problem is clearly in NP. Prove that this problem is NP-complete.

（試題隨試卷繳回）

教育部 112 年公費留學考試試題 105

科目：計算機程式 （全二頁，第一頁）

※可使用工程計算機(限僅具備＋、－、×、÷、% 、√、MR、MC、M+、M-、三角函數、對數、指數運算功能)。

※以中文或英文作答均可，評分基準相同。

※All of your implementations should be in C/C++, Python, or in pseudo-code that is easily comprehensible.

1. (15%) Explain the goal of the given Python and C++ programs, which yield identical outcomes. You only need to review one of the following programs based on your familiarity. What is the output for the input: n = 3620191, target = 16?

```python
# Python procedure
def MisteryInteger(self, n, target):
    n0 = n
    i = 0
    while sum(map(int, str(n))) > target:
        n = n // 10 + 1
        i += 1
    return n * (10 ** i) - n0
```

```cpp
// C++ procedure
int sum(long long n) {
        int res = 0;
        while (n) {
            res += n % 10;
            n /= 10; }
        return res;}
long long MisteryInteger(long long n, int target) {
        long long n0 = n, base = 1;
        while (sum(n) > target) {
            n = n / 10 + 1;
            base *= 10;
        }
        return n * base - n0;
    }
```

2. (15%) Implement a recursive procedure to find the depth of a binary tree. Design a non-recursive procedure for it.

3. (15%) You're given an array A of length n, where A[i] is the price of goods on the i-th day. Your task is to maximize the profit by choosing a single day to buy the goods and choosing a different day in the future to sell the goods. Return the maximum profit you can achieve from this transaction. If you cannot achieve any profit, return 0. Design a procedure for it and give the complexity of your method.

（接下頁）

4. (15%) Consider a single variable polynomial $P(x) = \sum_{i=1}^{n} a_i x^i$, where a_i's are the coefficients and x is a given value. Implement an efficient procedure to evaluate $P(x)$. What is the time complexity of your method?

5. (20%) Consider a fixed positive integer k and a sequence of real numbers $a_1, \ldots, a_k$, where $0 < a_i < 1$ for $1 \leq i \leq k$. Design an efficient procedure to find a real number r such that $\sum_{i=1}^{k} a_i^r = 1$ with precision within 10^{-6}. Explain why such r exists.

6. (20%) Consider a directed acyclic weighted graph $G = (V, E)$ and two distinct vertices s and t. Your task is to find a longest simple path from s to t. Design a dynamic programming procedure for this problem. What is the time complexity of your method?

教育部 112 年公費留學考試試題 106

科目：線性代數 （全一頁）

※可使用工程計算機(限僅具備＋、－、×、÷、% 、√、MR、MC、M+、M-、三角函數、對數、指數運算功能)

※以中文或英文作答均可，評分基準相同。

1. [15%] Is $T+c$ a linear transformation if T is a linear transformation from R^n to R^n for a non-zero constant c? A linear transformation always maps the origin to the origin, yes or no? Why?

2. [20%] Let $i=[1,0,0]$, $j=[0,1,0]$, and $k=[0,0,1]$. Confirm whether or not the set $B=\{i+j, i+k, 2k\}$ forms a basis of $\mathbb{R}^3$. In particular, can you find any possibility that the set B can generate $[1,1,1]$, i.e., $i+j+k$? Show how if it is possible.

3. [10%] Decide which one is bigger, E^2 or F for E and F are defined below? Why?
   $E=\mathbf{u}\cdot\mathbf{v}=(1.2 \quad 3.4 \quad 6.6)\cdot(2.2 \quad 4.4 \quad 7.6)$ and
   $F=\|\mathbf{u}\|^2\|\mathbf{v}\|^2=\|(1.2 \quad 3.4 \quad 6.6)\|^2\|(2.2 \quad 4.4 \quad 7.6)\|^2$.
   Note that " $\cdot$ " means an inner product.

4. [10%] Prove or disprove $(AB)^{-1}=B^{-1}A^{-1}$ for two $n\times n$ invertible matrices A and B.

5. [10%] Prove or disprove the statement, if the matrix A^2 is invertible, then so is A.

6. [25%] Evaluate $\lim_{n\to\infty} A^{2n}=\lim_{n\to\infty}\begin{bmatrix}-\frac{2}{3} & \frac{1}{3}\\ -\frac{7}{6} & \frac{5}{6}\end{bmatrix}^{2n}$ where $A=\begin{bmatrix}-\frac{2}{3} & \frac{1}{3}\\ -\frac{7}{6} & \frac{5}{6}\end{bmatrix}$. What is the result if we would like to find the form of A^{2n}?

7. [10%] Calculate $\det(AB)$ where A and B are given as follows:
   $A=\begin{bmatrix}1 & 4 & 5\\ 0 & 2 & 6\\ 0 & 0 & 3\end{bmatrix}$ and $B=\begin{bmatrix}-1 & 0 & 0\\ 5 & 1/3 & 0\\ 6 & 7 & 1/2\end{bmatrix}$.

（試題隨試卷繳回）

教育部 112 年公費留學考試試題 109

科目：資訊安全概論 （全二頁，第一頁）

※可使用工程計算機(限僅具備＋、－、×、÷、% 、√、MR、MC、M+、M-、三角函數、對數、指數運算功能)

一、(總分 25 分)在 COVID-19 疫情期間或是後疫情時代，員工遠距工作已漸成為常態。員工可利用 VPN(Virtual Private Network)技術在公共(public)不安全(unsecure)的網際網路(Internet)上建立安全的通訊連結，連線其電腦裝置到所屬企業的 VPN 主機，再連線到企業內網。通訊協定 IPsec 目前廣泛被用來實作 VPN。

(一) 請說明 IPsec 的 Authentication Header(AH)的主要功能為何？(10 分)

(二) 請問 AH 是如何運作以達到防止 IP address spoofing attack？(5 分)

(三) 請說明 AH 是如何可以防止 replay attack。(10 分)

二、(總分 25 分)在進階網路攻擊(Advanced Persistent Threat, APT)通常會歷經多個攻擊階段。首先，攻擊者於第一階段通常會先攻陷(compromise)目標網路的某一主機系統弱點(vulnerability)，入侵到目標網路。一般而言，攻擊者於攻陷的同時會夾帶所謂的 Dropper 或 RAT(remote access Trojan)軟體，請說明：

(一) Dropper 軟體的功能與作用。(8 分)

(二) RAT 軟體的功能與作用。(8 分)

(三) 請舉出兩種它們躲避主機系統偵察的做法。(9 分)

三、(總分 25 分)防火牆(Firewall)與入侵防禦系統(Intrusion Detection System, IDS)是目前企業網路資安防禦經常採用的設備。

(一) 防火牆的基本功用是執行企業的網路政策(policy)，也就是決定哪些外部 Internet 封包可以進到企業內網，與哪些企業內網的封包可以傳輸到 Internet。請問防火牆的存取控制列表(access control list)一般是檢查封包的哪些通訊協定層的標頭(header)內的欄位？(10 分)

(二) 入侵防禦系統使用惡意特徵庫(Signature set)檢查並阻擋帶有已知惡意內容的封包進入企業網路。請問惡意特徵庫的建立與維護有哪兩項重要的議題，攸關入侵防禦系統是否能在安全檢查的品質與效能上得到最好的效益。(15 分)

（接下頁）

教育部 112 年公費留學考試試題 109

科目：資訊安全概論 （全二頁，第二頁）

四、(總分 25 分)實務上，對稱式加密(symmetric encryption)、公開金鑰加密(public key infrastructure, PKI)，以及電子簽章(digital signature)方法被廣泛地應用在確保通訊之兩造雙方資料交換的機密性(confidentiality)、完整性(integrity)和身分認證(identity authenticity)。在網路銀行服務(e-banking)，如果客戶想要線上傳輸一重要文件到銀行端主機。請說明：

(一) 說明此文件該如何利用 PKI 技術達到雙方身分驗證(mutual authentication)並確保在網路上的安全傳輸，也就是傳輸內容不會被其它第三方看到。(8 分)

(二) 請問在認證銀行端主機的憑證是如何被認證？(10 分)

(三) 現在的資安身分認證(authentication)及加密(encryption)多仰賴 PKI 及非對稱加密演算法例如 Rivest-Shamir-Adleman (RSA)在後量子時代可能就無法再保護網路傳輸的安全性，引發資安疑慮，原因為何？(7 分)

（試題隨試卷繳回）

教育部112年公費留學考試試題 110

科目：離散數學 （全二頁，第一頁）

※可使用工程計算機(限僅具備＋、－、×、÷、% 、√、MR、MC、M+、M-、三角函數、對數、指數運算功能)

※以中文或英文作答均可，評分基準相同。

1. (15%) Which of the following statements are tautology?

   A. $[p \wedge (p \rightarrow q)] \rightarrow q$

   B. $[p \rightarrow (q \rightarrow r)]$

   C. $(p \wedge q) \rightarrow (p \vee q)$

   D. $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$

2. (10%) If three integers are selected, at random and without replacement, from {1,2,3,…,99,100}, what is the probability such that their sum is even ?

3. (10%) For three sets A,B, and C, please simplify the following set expression $\overline{\overline{(A \cup B) \cap C} \cup \overline{B}}$.

4. (15%) For what base do we find that 251+445=1026.

5. (24%) Let $A=\{1,2,3,4\}$ and $B=\{x,y,z\}$.

   A. (3%) List three functions from A to B.

   B. (3%) How many functions $f: A \rightarrow B$ are there?

   C. (3%) How many functions $f: A \rightarrow B$ are one-to-one?

   D. (3%) How many functions $g: B \rightarrow A$ are there?

   E. (3%) How many functions $g: B \rightarrow A$ are one-to-one?

   F. (3%) How many functions $f: A \rightarrow B$ satisfy $f(1)=x$?

   G. (3%) How many functions $f: A \rightarrow B$ satisfy $f(1)=f(2)=x$?

   H. (3%) How many functions $f: A \rightarrow B$ satisfy $f(1)=x$ and $f(2)=y$?

6. (16%) Find the generating function for the following sequences:

（接下頁）

A. (3%) 0,1,0,0,0,…

B. (3%) 0,1,1,1,1,…

C. (3%) 0,1,2,3,4,…

D. (3%) 0,1,3,6,10,…

E. (4%) Use the above result 6D to find a formula for $\sum_{k=1}^{n} k$.

7. (10%) The chromatic number of a graph is the minimum number of colors needed to label the vertices so that adjacent vertices receive different colors. Please determine the chromatic number of a bipartite graph.

教育部 112 年公費留學考試試題 111

科目：半導體物理 **（全二頁，第一頁）**

※可使用工程計算機(限僅具備＋、－、×、÷、% 、√、MR、MC、M+、M-、三角函數、對數、指數運算功能)。

※以中文或英文作答均可，評分基準相同。

一、 (25%) For a *n*-Si crystal doped with donor atoms with a donor electron energy state of E_d, the Fermi level E_F is located at $E_F - E_c = -0.2$ eV, where E_c is the energy of conduction band edge. It is known that at room temperature, Si E_g = 1.12 eV, 1 kT/q = 0.0259 V, $q = 1.6\times10^{-19}$ C.

(a) For an energy state in conduction band with an energy level of $E_{t1} - E_c = 0.1$ eV, find the electron occupancy possibility of the state E_{t1} at room temperature. (7 %)

(b) For an energy state in valence band with an energy level of $E_{t2} - E_v = -0.1$ eV, find the hole occupancy possibility of the state E_{t2} at room temperature. E_v is the energy of valence band edge. (8 %)

(c) At room temperature, list the high low relationship among the energy levels of E_c, E_v, E_F, E_d, and E_{Fi}. (5 %)

(d) At absolute zero temperature (0 K), list the high low relationship among the energy levels of E_c, E_v, E_F, E_d, and E_{Fi}. (5 %)

二、 (25%) For an ideal Si *pn* junction, the doping concentrations in *p* and *n* regions are $N_A = 4\times10^{13}$ cm^{-3} and $N_D = 8\times10^{13}$ cm^{-3} respectively. It is known that at room temperature 1 kT/q = 0.0259 V, $q = 1.6\times10^{-19}$ C, Si $n_i = 1.5\times10^{10}$ cm^{-3}, $\varepsilon_{Si} = 11.9$ ε_o, $\varepsilon_o = 8.85\times 10^{-14}$ F/cm, Si electron and hole mobility are $\mu_n = 1350$ cm^2/v·s and $\mu_p = 480$ cm^2/v·s respectively, $D/\mu = kT/q$. Assume the minority carrier lifetimes in *p* and *n* regions are τ_n =1 μs and τ_p =2 μs. Ignore the effect of net generation-recombination mechanism in depletion region when the device is under non-equilibrium condition.

(a) Under thermal equilibrium, find the built-in potential V_{bi} = ? (5%)

(b) Under a forward bias of V_F = 0.2V, find the ideal current density J = ? (6 %)

(c) Let x_n be the position of the depletion edge in x region. Under a forward bias of V_F = 0.2V, find the product of the electron and hole concentrations at x_n ? (6 %)

(d) Under a reverse bias of $V_R = -4$ V, find the total depletion width W_D = ? Also, find the small signal junction capacitance C_j = ? (8 %)

（接下頁）

教育部 112 年公費留學考試試題 111

科目：半導體物理 （全二頁，第二頁）

三、 (25%) For a practical *pn* junction, the effect of net generation or net recombination mechanism should be considered in depletion region under a certain bias.

(a) Plot the schematic distributions of the quasi Fermi levels of electron E_{Fn} and hole E_{Fp} within the whole *pn* junction under forward and reverse bias conditions. (8 %)

(b) Which mechanism mentioned above dominates the current in forward bias condition? Similarly, which mechanism in reverse bias condition? (6 %)

(c) What are the 1 kT current and 2 kT current? (6 %)

(d) What is the ideality factor of a practical *pn* junction? (5 %)

四、 (25%) In a metal/oxide/semiconductor MOS structure, the SiO_2 oxide thickness is 250 nm and the doping concentration of *p*-Si is $N_A = 2\times10^{14}$ cm^{-3}. It is known that $\varepsilon_{SiO2} = 3.9\ \varepsilon_o$, $\varepsilon_o = 8.85\times 10^{-14}$ F/cm. At room temperature 1 $kT/q = 0.0259$ V, $q = 1.6\times10^{-19}$ C, Si $n_i = 1.5\times10^{10}$ cm^{-3}. The interface trap density D_{it} of 2×10^{11} cm^{-2}eV^{-1} at SiO_2/Si interface is considered. Assume the D_{it} are acceptor-like for $E_t > E_{Fi}$ and donor-like for $E_t < E_{Fi}$, and are constant in density within the bandgap at interface, where E_t is the energy level of D_{it} trap.

(a) Find the value of E_{Fi}-E_F in thermal equilibrium of *p*-Si bulk substrate, where E_{Fi} is the intrinsic Fermi level and E_F the Fermi level of *p*-Si. (8 %)

(b) At flat-band condition, find the total effective interface charges Q_{it}/q due to D_{it}? Also, find the flat-band voltage shift $\triangle V_{FB}$ due to D_{it}. (12 %)

(c) When the MOS was biased to the condition that the Si surface is intrinsic, find the total effective interface charges Q_{it}/q due to D_{it}? (5 %)

（試題隨試卷繳回）

教育部 112 年公費留學考試試題 112

科目：電子學 （全三頁，第一頁）

※可使用工程計算機(限僅具備＋、－、×、÷、% 、√、MR、MC、M+、M-、三角函數、對數、指數運算功能)

※以中文或英文作答均可，評分基準相同。

1. (20%) For the circuits given in Figure 1(a) & 1(b), assume that the NMOS is biased at saturation mode with

$|v_t| = 0.6$ V, $\lambda = 0.01$ V^{-1}, $\gamma = 0$, $\mu_n C_{ox} = 100$ μA/V^2

$L = 1$ μm and $W = 2$ μm. Please calculate

(a)$g_m \times r_o$ of Figure 1(a) [10%]

(b)small-signal voltage gain v_o/v_i of Figure 1(b) [10%]

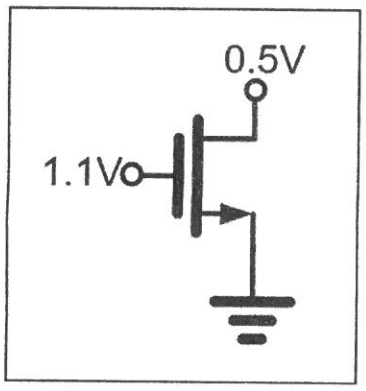


Figure 1(a)

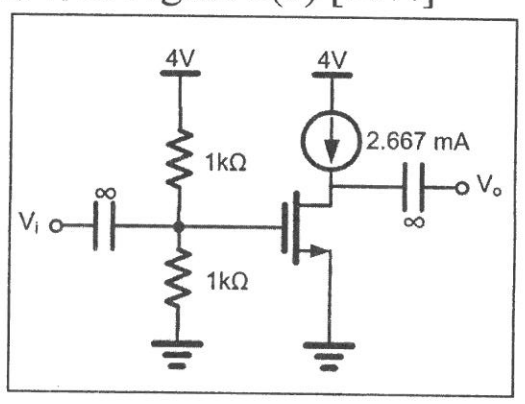


Figure 1(b)

2. (10%) In the capacitor-coupled circuit shown in Figure 2, current of the diodes are $I_d = I_S \exp(V_d / 2V_T)$, $V_T = 25$ mV.

For small input signals, what value of resistor R is needed for $v_o/v_i = 0.5$?

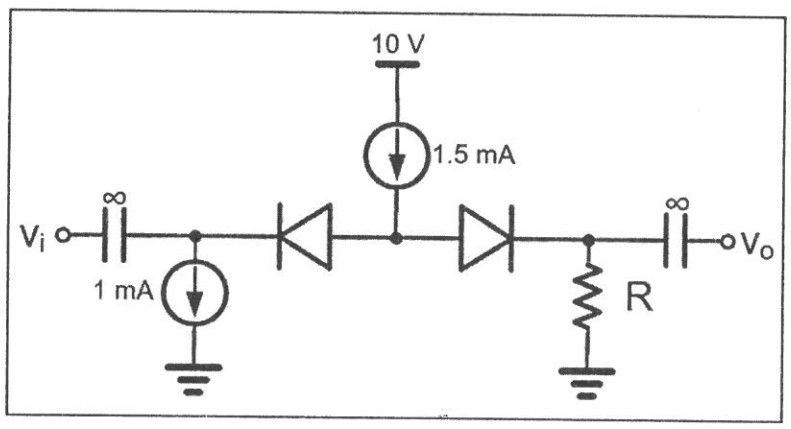
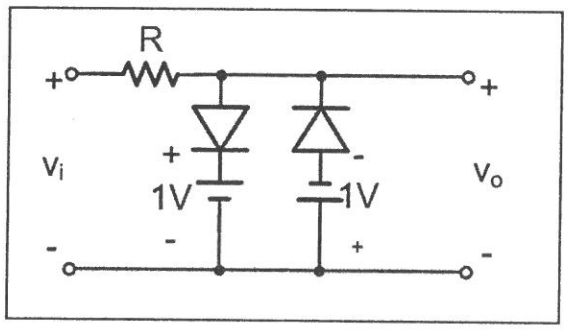


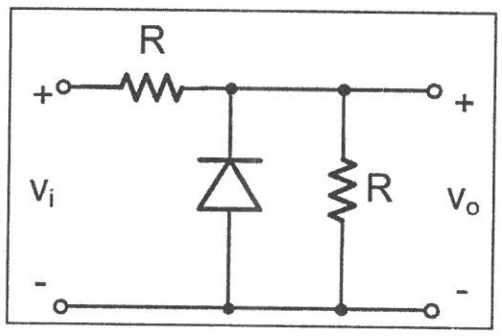
Figure 2

（接下頁）

3. (20%) For the circuits given in Figure 3(a) & Figure 3(b), assume $V_D = 0.7$ V. Please sketch a plot showing the relationship between v_i and v_o like Figure 3(c).



(10%) Figure 3(a)



(10%) Figure 3(b)

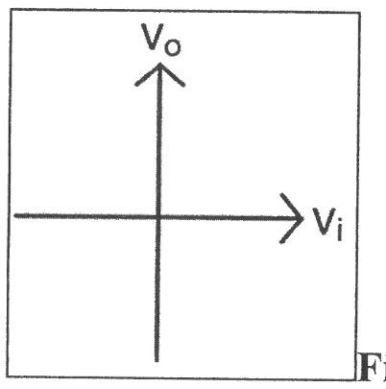


Figure 3(c)

4. (20%) For the circuit given in Figure 4, assume $\beta = 100$, I_C=1 mA, V_T=25 mV and neglect the Early effect.

Please calculate

(a) g_m =? mA/V [10%]

(b) A_v =? V/V [10%]

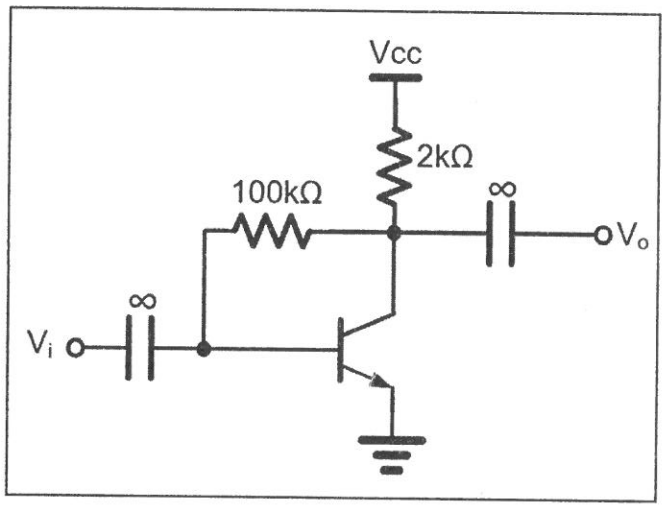


Figure 4

（接下頁）

5. (10%) Refer to Figure 5. Given the following data, calculate G_m, R_o, and A_{v0} for the circuit.

$I= 200\ \mu A$, $\beta = 125$, $\mu_n C_{ox}= 400\ \mu A/V$, $W/L= 25$, $V_A= 1.8\ V$, $V_T = 25mV$.

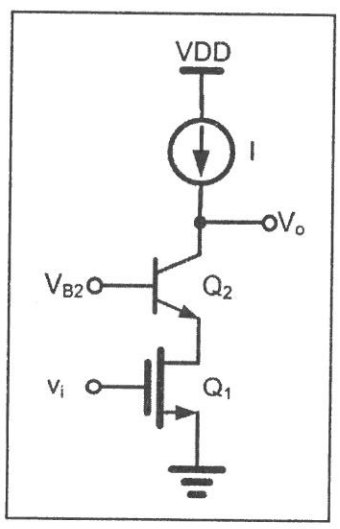


Figure 5

6. (20%) For the circuit in Figure 6, assume an ideal op amp.

(a)Use superposition to find v_o in terms of the input voltage v_1 and v_2. [10%]

(b)For

$$v_1 = 2\sin(2\pi\times 10t) - 0.5\sin(2\pi\times 200t), \text{volts}$$

$$v_2 = 4\sin(2\pi\times 10t) + 0.5\sin(2\pi\times 200t), \text{volts}$$

find v_o. [10%]

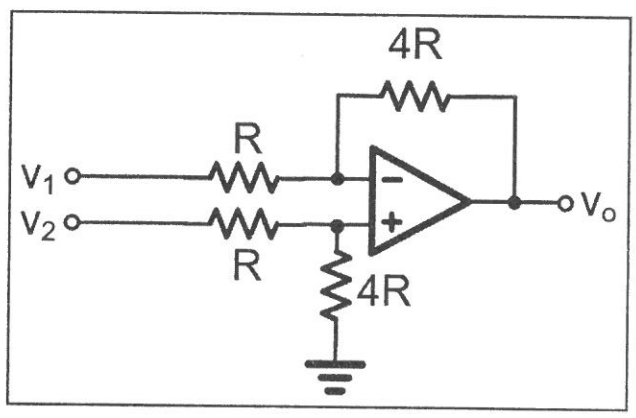


Figure 6