OLD DOMINION UNIVERSITY
PH.D. DIAGNOSTIC EXAM
Spring 2024

ODU HONOR PLEDGE

I pledge to support the Honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community, it is my responsibility to turn in all suspected violators of the Honor Code. I will report to a hearing if summoned.

Student Signature: _____

Student Name (BLOCK CAPITALS): _____

UIN Number: _____

Please turn in this examination document with the pledge above signed and with one answer book for each solved problem.

1. This examination contains 30 problems in the following seven areas:

A.	MATH (At most 3 problems can be answered from the Math area)	A1	A2	A3	A4		
B.	CIRCUITS & ELECTRONICS	B1	B2	B3			
C.	SYSTEMS, SIGNAL AND IMAGE PROCESSING	C1	C2	C3	C4	C5	C6
D.	PHYSICAL ELECTRONICS I	D1	D2	D3			
E.	PHYSICAL ELECTRONICS II	E1	E2	E3			
F.	COMPUTER SYSTEMS	F1	F2	F3	F4	F5	F6
G.	CYBERSECURITY	G1	G2	G3	G4	G5	

2. You must answer eight problems (no more than three from the MATH group).
3. Answer in the blue books provided. **Use a separate book for each problem. Put the title and problem number on the front of each book (eg., MATH A-1)**
4. Return all the 30 problems.
5. You will be graded on your answers to eight problems only**.**
6. The examination is "closed-book;" only blue books, exam problems and a scientific calculator are allowed. **No formula sheet is allowed**. Some problems include reference formulas. No material shall be shared without prior permission of the proctor(s).
7. You have four hours to complete this examination.

PROBLEM A1 – MATH

In the complex plane, compute the contour integral along the curve C of the function $f(z)=\sin(z)/(z^2+1)$, where C is the unit circle $|z|=1$ traversed counterclockwise.

PROBLEM A2 – MATH

Consider a triangle T whose vertices are $(0,0), (1,1), (2,0)$ Evaluate the surface integral

$$\int_T dxdy\,(x+y)^2$$

PROBLEM A3 – MATH

Linear Algebra

Let A be a real-valued matrix with dimensions $m \times n$ and linearly independent columns, and consider the linear system of equations $A\underline{x} = \underline{b}$, where $\underline{b} \in \mathbb{R}^m$ is a given vector.

1. Assuming that the system has no solutions, that is, there exists no vector $\underline{x} \in \mathbb{R}^n$ such that $A\underline{x} = \underline{b}$, explain how the "least squares" solution $\hat{x}$ is found and determine the expression of $\hat{x}$.
2. Write the expression of the projection matrix P_A onto the subspace defined by the matrix A and show that $(P_A)^k = P_A$ for any integer $k \geq 2$.

Note: For full credit formal proofs using a sequence of logical reasoning steps are expected.

PROBLEM A4 – MATH

Probability

A wide-sense stationary process $\boldsymbol{x}(t)$ with autocorrelation function $R_x(\tau) = 1 + \delta(\tau)$ is filtered by a linear time-invariant system with impulse response $h(t) = \mathrm{e}^{-t}u(t)$, where $u(t)$ denotes the unit step function. Let $\boldsymbol{y}(t)$ be the filter's output. Compute the following:

(a) the power spectrum of $\boldsymbol{x}(t)$, $S_x(\omega)$;

(b) the cross power spectrum $S_{xy}(\omega)$;

(c) $S_y(\omega)$;

(d) $R_y(\tau)$;

(e) $E[\boldsymbol{y}^2(t)]$.

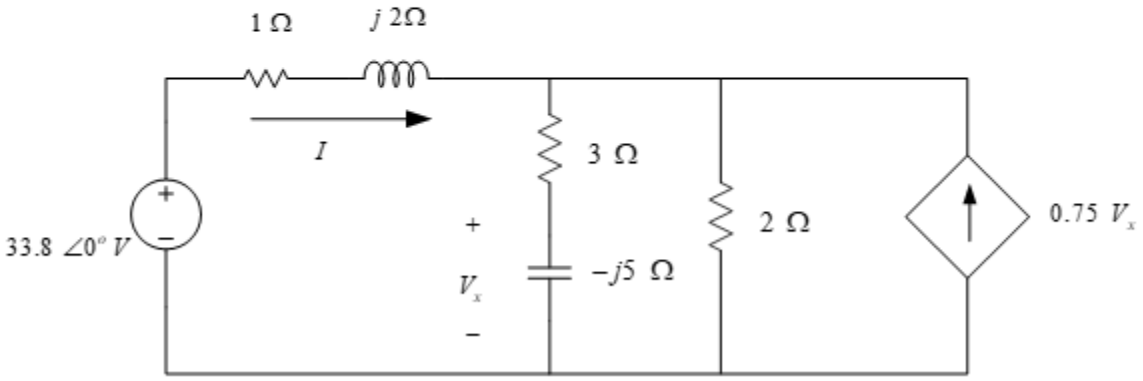
TABLE 7.1 Select Fourier Transform Pairs

No.	$x(t)$	$X(\omega)$	
1	$e^{-at}u(t)$	$\frac{1}{a+j\omega}$	$a>0$
2	$e^{at}u(-t)$	$\frac{1}{a-j\omega}$	$a>0$
3	$e^{-a\lvert t\rvert}$	$\frac{2a}{a^2+\omega^2}$	$a>0$
4	$te^{-at}u(t)$	$\frac{1}{(a+j\omega)^2}$	$a>0$
5	$t^n e^{-at}u(t)$	$\frac{n!}{(a+j\omega)^{n+1}}$	$a>0$
6	$\delta(t)$	1	
7	1	$2\pi\delta(\omega)$	
8	$e^{j\omega_0 t}$	$2\pi\delta(\omega-\omega_0)$	
9	$\cos\omega_0 t$	$\pi[\delta(\omega-\omega_0)+\delta(\omega+\omega_0)]$	
10	$\sin\omega_0 t$	$j\pi[\delta(\omega+\omega_0)-\delta(\omega-\omega_0)]$	
11	$u(t)$	$\pi\delta(\omega)+\frac{1}{j\omega}$	
12	$\operatorname{sgn} t$	$\frac{2}{j\omega}$	
13	$\cos\omega_0 t\,u(t)$	$\frac{\pi}{2}[\delta(\omega-\omega_0)+\delta(\omega+\omega_0)]+\frac{j\omega}{\omega_0^2-\omega^2}$	
14	$\sin\omega_0 t\,u(t)$	$\frac{\pi}{2j}[\delta(\omega-\omega_0)-\delta(\omega+\omega_0)]+\frac{\omega_0}{\omega_0^2-\omega^2}$	
15	$e^{-at}\sin\omega_0 t\,u(t)$	$\frac{\omega_0}{(a+j\omega)^2+\omega_0^2}$	$a>0$
16	$e^{-at}\cos\omega_0 t\,u(t)$	$\frac{a+j\omega}{(a+j\omega)^2+\omega_0^2}$	$a>0$
17	$\operatorname{rect}\left(\frac{t}{\tau}\right)$	$\tau\operatorname{sinc}\left(\frac{\omega\tau}{2}\right)$	
18	$\frac{W}{\pi}\operatorname{sinc}(Wt)$	$\operatorname{rect}\left(\frac{\omega}{2W}\right)$	
19	$\Delta\left(\frac{t}{\tau}\right)$	$\frac{\tau}{2}\operatorname{sinc}^2\left(\frac{\omega\tau}{4}\right)$	
20	$\frac{W}{2\pi}\operatorname{sinc}^2\left(\frac{Wt}{2}\right)$	$\Delta\left(\frac{\omega}{2W}\right)$	
21	$\sum_{n=-\infty}^{\infty}\delta(t-nT)$	$\omega_0\sum_{n=-\infty}^{\infty}\delta(\omega-n\omega_0)$	$\omega_0=\frac{2\pi}{T}$
22	$e^{-t^2/2\sigma^2}$	$\sigma\sqrt{2\pi}e^{-\sigma^2\omega^2/2}$	

PROBLEM B1 – CIRCUITS AND ELECTRONICS

Sinusoidal Steady State Response

Use the mesh-current method to find the phasor current I in the following circuit. Use phasor analysis. What is the power dissipated in the 1Ω resistor?

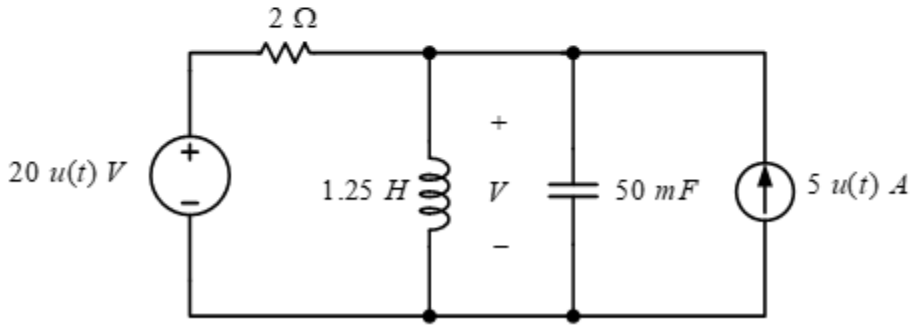


PROBLEM B2 – CIRCUITS AND ELECTRONICS

Laplace Application to Circuit Analysis - Superposition

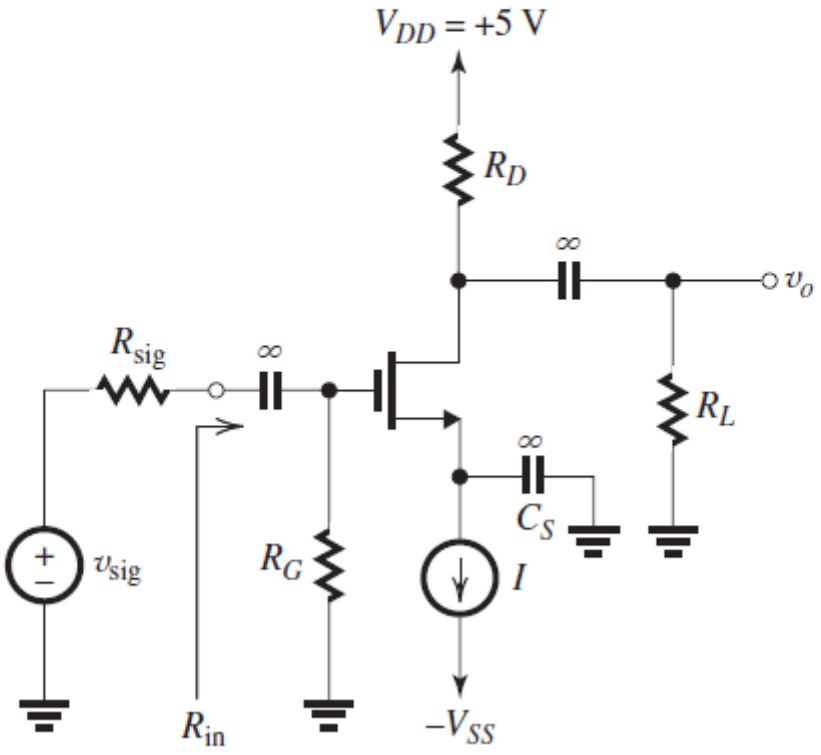
There is no energy stored in the circuit shown at the time the two sources are turned on.

a. Draw the Laplace Transformed equivalent circuit in *s-domain*.
b. Find the *s-domain* expression for the voltage component $V'(s)$,due to the voltage source 20 u(t) V only.
c. Find the *s-domain* expression for the voltage component $V''(s)$,due to the current source - 5 u(t) A only.
d. Using the principle of superposition, find the time domain expression for v(t) for t > 0.



PROBLEM B3 – CIRCUITS AND ELECTRONICS

The MOSFET in the below circuit has $\mu_n C_{ox}(W/L) = 4\text{mA/V}^2$.
(a) Find the value of I that causes the MOSFET to operate in saturation with an overdrive voltage of 0.25V.
(b) What value of R_D results in $V_D = 0\text{V}$?
(c) Find the value of g_m.
(d) Find the value of r_o given that $V_A = 25\text{V}$.



PROBLEM C1 – SYSTEMS, SIGNALS AND IMAGE PROCESSING

Image processing

1.

a. Use your own words to describe Notch Filtering. Should we use Notch Filtering on images with or without correlated noise? Why?

b. Which of following spectrum power image is the most likely to have a correlated noise? Why?

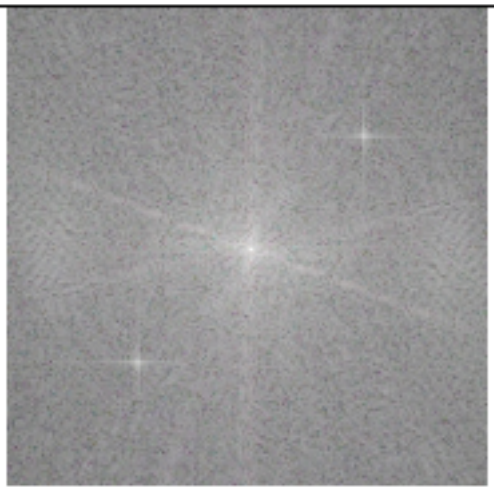


Image A	Image B

2.

a. Explain Histogram Equalization.

b. Given the following 3x3 image I (grey image), you need to conduct Histogram Equalization on it and show each step to get the result.

Hint: $\mathbf{J}(r,c,b) = 255 \cdot P_{\mathbf{I}}\left[\mathbf{I}(r,c,b)+1\right]$, where $P_{\mathbf{I}}$ is the cumulative distribution function (CDF) of image, *I*.

100	11	11
100	255	11
50	50	11

Intensity Values for 3x3 Image, *I*

PROBLEM C2 – SYSTEMS, SIGNALS AND IMAGE PROCESSING

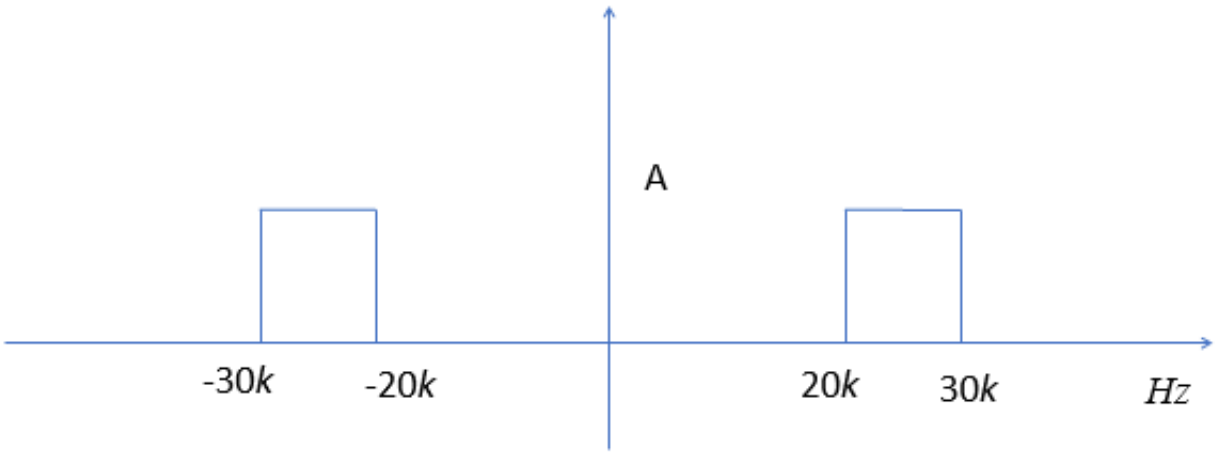
A causal LTID system is characterized by the following difference equation:

$$y[n] - \frac{3}{4}y[n-1] + \frac{1}{8}y[n-2] = x[n]$$

(a). Determine the system function H(z) for the system (2 points)
(b). Determine the impulse response $h[n]$ for the LTI system (2 points).
(c). Is the system stable? Is the system causal? Justify your answer (2 points).
(d). If $x[n] = (1/3)^n u[n]$, what is $y[n]$ (2 points)?
(e). If $x[n] = 2\sin(\pi n + \pi/2)$, what is $y[n]$ (2 points)?

PROBLEM C3 – SYSTEMS, SIGNALS AND IMAGE PROCESSING

(10 points) An analog signal, $x(t)$, has a spectrum as shown below.



a) (2 points) What is the Nyquist rate for $x(t)$?
b) (5 points) Assume that you sampled the analog signal, $x(t)$, using a sampling frequency of $120k$ Hz and obtained a discrete-time sequence $x[n]$, draw the spectrum of $x[n]$ for three periods.
c) (3 points) What is the highest frequency component in the above resulted discrete-time sequence $x[n]$ in Q2 b)?

PROBLEM C4 – SYSTEMS, SIGNALS AND IMAGE PROCESSING

A possible configuration for a hybrid electric vehicle is shown in Figure 1.

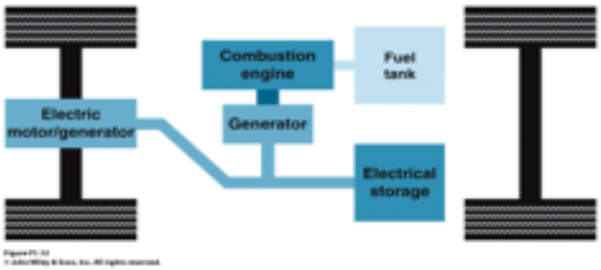


Figure 1. A series connected hybrid electric vehicle.

Suppose that the electric motor is an armature controlled DC motor and that it is the only source of power. Under these conditions, a block diagram of the electrical motor system is shown in Figure 2, where

- $\omega(t)$ = motor's angular speed = the output
- $u_c(t)$ = voltage generated by the electronic control unit, driving a power amplifier that produces a reference voltage, and
- $T_c(t)$ = load torque that depends on the vehicle dynamics.

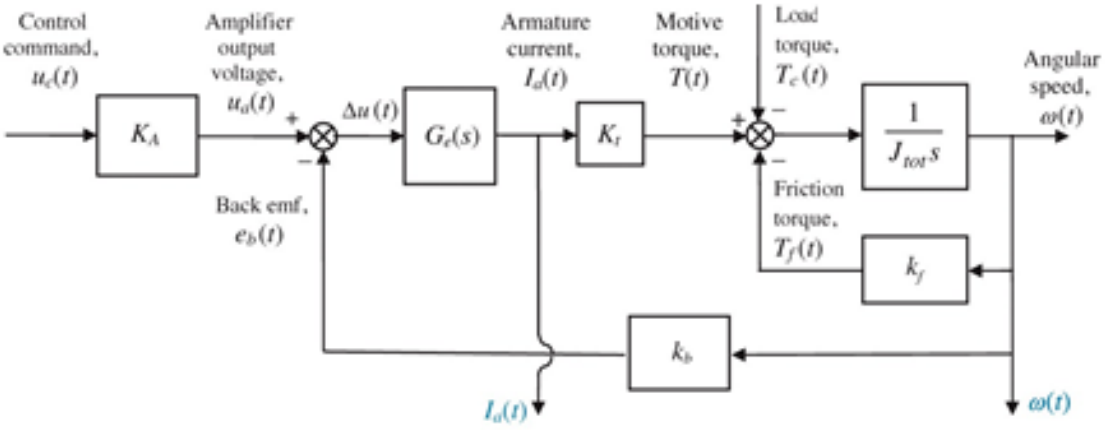


Figure 2. Block diagram representation of the electrical subsystem.

a) Use superposition to find the input-output transfer functions

$$\frac{\mathcal{L}\{\omega(t)\}}{\mathcal{L}\{u_c(t)\}} \text{ and } \frac{\mathcal{L}\{\omega(t)\}}{\mathcal{L}\{T_c(t)\}}.$$

For control purposes, suppose that the vehicle's output is the forward velocity, that the input is $u_c(t)$, that a proportional controller with gain K is being used and that the transfer function of this system is given by

continuted on next page

$$G(s)=\frac{K(s+0.6)}{(s+0.5)(s+0.02)}.$$

b) If the closed-loop system is critically damped when $K\approx 0.2$ and $K\approx 1.16$ show the root locus plot and determine the approximate range of values for $K>0$ that result in underdamped response.

c) When $K=1$ what is the steady-state error, the approximate settling time, and the approximate percent overshoot?

d) If it is determined that the settling time is too long, describe a detailed procedure to change the current closed loop system to reduce the settling time by a factor of 10.

REVIEW

For a prototype second order open-loop transfer function $G(s) = \omega_n^2/(s^2 + 2\zeta\omega_n s + \omega_n^2)$ the following unit step response relations are useful:

- percent overshoot = $100 \exp(-\zeta\pi / \text{sqrt}(1 - \zeta^2))$
- 2% settling time $\approx 4 / (\zeta\omega_n)$

Suppose that the loop gain of the closed-loop system can be written as $KG(s)$ with

$G(s)=K_G\dfrac{\prod_{i=1}^{m}(s-z_i)}{\prod_{j=1}^{n}(s-p_j)}$, where K is the gain of the controller that needs to be determined, $G(s)$ represents the loop gain when K=1, and the loop gain has m zeros at z_i and n poles at p_j. The magnitude condition of root locus states that

$$|K|=\frac{\prod_{j=1}^{n}|s-p_j|}{K_G\left(\prod_{i=1}^{m}|s-z_i|\right)},\quad \text{whenever } s \text{ a closed-loop pole}.$$

Laplace's Theorems

Let F(s) be the Laplace transform of f(t).

- Initial Value Theorem
  - Now, if $F(s)$ be a strictly proper rational transfer function (degree denominator > degree numerator), then

$$f(0^+)=\lim_{s\to\infty} sF(s).$$

- Final Value Theorem
  - If all the poles of $sF(s)$ have negative real parts, then

$$\lim_{t\to\infty} f(t)=\lim_{s\to 0} sF(s).$$

PROBLEM C5 – SYSTEMS, SIGNALS AND IMAGE PROCESSING

Communications Problem:

1. Define signal multiplexing and explain what is the difference between frequency division multiplexing (FDM) and time division multiplexing (TDM). Which of these two multiplexing methods cannot be used with analog signals? Explain why.
2. Explain what quadrature-carrier multiplexing is and how it works by sketching block diagrams of the corresponding transmitter and receiver, writing the expression of multiplexed transmitted signal, and showing how the distinct signals are separated at the receiver.

For full credit the explanations should be given in full sentences with sufficient details, and should include all supporting arguments.

PROBLEM C6 – SYSTEMS, SIGNALS AND IMAGE PROCESSING

Communications Networks:

1. (5 pts) We have a character frame from the higher layer: A FLAG ESC B C. Assume the byte stuffing framing method is used at the data link layer, what will be the actual frame to be transmitted? Note the special characters are FLAG and ESC.

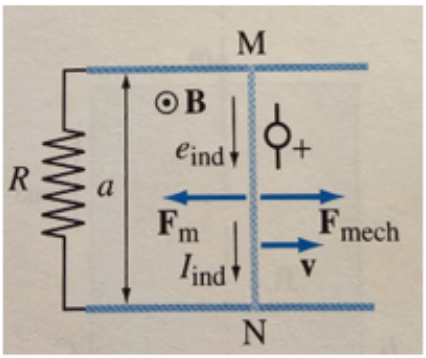
2. (5 pts) Consider a signal transmitted over a 30KHz channel. If the SNR is 30 dB, what is the maximum achievable rate?

PROBLEM D1 – PHYSICAL ELECTRONICS I

A 60 - MHz plane wave traveling in the **negative** x -direction in dry soil with relative permittivity $\epsilon_r = 4$ has an electric field polarized along the z - direction. Assuming dry soil to be approximately lossless, and given that the magnetic field has a peak value of 10 (mA/m) and that its value was measured to be 7 (mA/m) at $t = 0$ and $x = -0.75$ m, develop complete expressions for the wave's electric and magnetic fields, $\vec{E}(x, t)$ and $\vec{H}(x, t)$.

PROBLEM D2 – PHYSICAL ELECTRONICS I

A metallic bar of length a=2m slides without friction at a constant velocity over parallel metallic rails, as shown in below figure. The bar is perpendicular to the rails and the mechanical force acting on the bar is $F_{mech} = 4N$. The whole system is situated in a uniform time-invariant magnetic field of flux density B = 1 T. The field lines are perpendicular to the plane of the rails and directed out of the page. A load of resistance R = 5Ω is connected between the rails. The losses in the bar and in the rails, as well as the magnetic field due to induced currents in the system, can be neglected. Evaluate the power of Joule's losses in the load and discuss the energy balance in this system.



PROBLEM D3 – PHYSICAL ELECTRONICS I

Optical fiber communications

The V-parameter of a planar fiber is given by:

$$V = (\pi d/\lambda_o).(n_1^2 - n_2^2)^{1/2}$$

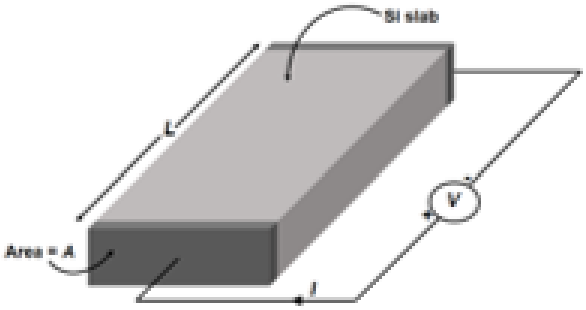
Where n_1 and n_2 are the refractive indexes of the core and the cladding, respectively, d is the thickness of the core, and λ_o is the wavelength of the light. If the number of modes that can travel down the fiber is given by N = 1 + INT(2V/π),

1. Derive the condition for a single mode fiber in terms of n_1, n_2, d, and λ_o.
2. For n_1 = 1.48, n_2 = 1.46, and λ_o = 1 μm, calculate the maximum core thickness, d, to have single mode propagation.

PROBLEM E1 - PHYSICAL ELECTRONICS II

Solid State Electronics (modified from Cornell ECE Open Courseware, ECE 3150)

A piece of p-doped silicon (doping concentration 6×10^{24} m^{-3}) with an area $A = 1 \times 10^{-12}$ m^2 and length $L = 1 \times 10^{-5}$ m. If the hole diffusivity $D_p = 27 \times 10^{-4}$ m^2/s, calculate the resistance of this piece at room temperature (kT = 0.026 eV at room temperature, where k is Boltzmann's constant and T temperature; Electron charge = 1.6×10^{-19} C)



PROBLEM E2 – PHYSICAL ELECTRONICS II

Physical electronics

1. Germanium has a diamond crystal structure (similar to silicon). Assume the lattice constant for Germanium is 0.937 at 300 K. Calculate the number of Germanium atoms per cubic centimeter and the density of Germanium at room temperature.

2. In an n-type semiconductor at T = 300 K, the electron concentration varies linearly from 10^{17} to 3×10^{16} cm^{-3} over a distance of 0.72 cm. Calculate the diffusion current density if the electron diffusion coefficient is 268 cm^2/s.

3. An ideal silicon junction has $N_A = 2 \times 10^{19}$ cm^{-3} and $N_D = 4 \times 10^{15}$ cm^{-3}. Calculate the depletion layer width, the maximum field and the junction capacitance at zero volt and at reverse bias of 3V (T = 300K).

   A list of equations and data is provided to you below. Please note that not all equations and data should be used.

$$J_n = q\mu_n n\mathscr{E} + qD_n \frac{dn}{dx} \qquad \frac{d^2\psi}{dx^2} \equiv -\frac{d\mathscr{E}}{dx} = -\frac{\rho_s}{\varepsilon_s} = -\frac{q}{\varepsilon_s}\left(N_D - N_A + p - n\right).$$

$$V_{bi} = \psi_n - \psi_p = \frac{kT}{q}\ln\left(\frac{N_A N_D}{n_i^2}\right). \qquad N_A x_p = N_D x_n. \qquad W = x_p + x_n.$$

$$\mathscr{E}_m = \frac{qN_D x_n}{\varepsilon_s} = \frac{qN_A x_p}{\varepsilon_s}. \qquad V_{bi} = \frac{1}{2}\mathscr{E}_m W. \qquad W = \sqrt{\frac{2\varepsilon_s}{q}\left(\frac{N_A + N_D}{N_A N_D}\right)V_{bi}}.$$

$$\mathscr{E}(x) = -\mathscr{E}_m + \frac{qN_B x}{\varepsilon_s}, \qquad \mathscr{E}_m = \frac{qN_B W}{\varepsilon_s}$$

$$C_j = \frac{\varepsilon_s}{W} = \sqrt{\frac{q\varepsilon_s N_B}{2(V_{bi} - V)}} \qquad V_{bi} = \frac{kT}{q}\ln\frac{p_{po}n_{no}}{n_i^2} = \frac{kT}{q}\ln\frac{n_{no}}{n_{po}},$$

$$n_{no} = n_{po}e^{qV_{bi}/kT}. \qquad D_n = \left(\frac{kT}{q}\right)\mu_n$$

$$p_{po} = p_{no}e^{qV_{bi}/kT}. \qquad n_n = n_p e^{q(V_{bi}-V)/kT}, \qquad n_p = n_{po}e^{qV/kT}$$

$$J = J_p(x_n) + J_n(-x_p) = J_s\left(e^{qV/kT} - 1\right), \qquad J_s \equiv \frac{qD_p p_{no}}{L_p} + \frac{qD_n n_{po}}{L_n},$$

Silicon (300 K): $N_C = 2.86\ 10^{19}$ cm^{-3} ; $N_V = 2.66\ 10^{19}$ cm^{-3} ; $n_i = 9.65\ 10^9$ cm^{-3}

$m_p = 1\ m_0$; $m_n = 0.19\ m_0$; $m_0 = 0.91\ 10^{-30}$ kg; $k = 1.38\ 10^{-23}$ J/K ; $q = 1.6\ 10^{-19}$ C

PROBLEM E3 – PHYSICAL ELECTRONICS II

Plasma (modified from M. Lieberman, A. Lichtenberg, Principles of Plasma Discharges and Materials Processing)

(1) A weakly ionized plasma having a Maxwellian electron distribution, which is

$$f_e(v) = \left(\frac{m}{2\pi e T_e}\right)^{3/2} e^{-\varepsilon/T_e}$$

With electron energy $\varepsilon = \frac{1}{2} m v^2 / e$ and electron temperature T_e both are in Volts, and with the normalization

$$4\pi \int_0^\infty v^2 \, dv \, f_e(v) = 1$$

Find the rate coefficients $K(T_e)$ for T_e = 2 Volts, for the Maxwellian electron collisions with stationary neutral gas molecules when the collision cross section σ is constant with a value:

$$\sigma = 10^{-20} m^2$$

PROBLEM F1 – COMPUTER SYSTEMS

Microprocessors

You are designing a system to compute the frequency of an input signal S. The frequency of the input is in the range from 1MHz to 100MHz. You can assume a peripheral that that directly receives S, outputs a pulse when the signal changes from a `'0'` to `'1'`. You can assume the following:

- Timers
- Free running counters
- Counters
- Watchdog timers (sometimes referred to as a COP timer)
- hex digit display with 8 digits
- The system clock frequency is 1GHz

You may used the assembly code listed on the next page or any assembly code for an alternate processor you are familiar with to solve this problem. If your solution is based on an alternate processor, please indicate which you are using.

1. (2 points) Describe the differences between polled I/O and interrupt based I/O. For each, give one advantage and one disadvantage.
2. (3 points) Give a block diagram of your system including the CPU, memory, and peripherals. You may assume the peripherals are accessed using memory mapped I/O. Provide address assignments for the peripherals.
3. (5 points) Give the pseudocode (partial credit) or assembly (full credit) for the assembly language program that computes the frequency and displays it on the hex display to a precision of two decimal points. State any assumptions you make regarding the operation of the peripherals.

Continued on next page

Category	Instruction				Low power	Meaning
Arithmatic	addi	rB,	rA	imm[1]		rB ← rA + imm_S
	add	rC,	rA,	rB		rC ← rA + rB
	sub	rC,	rA,	rB		rC ← rA − rB
	muli	rC,	rA,	rB		rC ← (rA × imm_S)$_{31..0}$
	mul	rC,	rA,	rB		rC ← (rA × rB)$_{31..0}$
	mulxuu	rC,	rA,	rB		rC ← ((unsigned)rA × (unsigned)rB)$_{63..32}$
Logical	and	rC,	rA,	rB		rC ←rA *and* rB
	andi	rB,	rA,	imm	y	rB ←rA *and* imm_U
	or	rC,	rA,	rB		rC ←rA *or* rB
	ori	rB,	rA,	imm	y	rB ←rA *or* imm_U
	xor	rC,	rA,	rB		rC ←rA *xor* rB
	xori	rB,	rA,	imm	y	rB ←rA *xor* imm_U
	nor	rC,	rA,	rB		rC ←rA *nor* rB
Comparator	cmpgai	rB,	rA,	imm		rB ← (rA ≥ imm_S)? 1 : 0
	cmplti	rB,	rA,	imm		rB ← (rA < imm_S)? 1 : 0
	cmpnai	rB,	rA,	imm		rB ← (rA ≠ imm_S)? 1 : 0
	cmpeqi	rB,	rA,	imm		rB ← (rA = imm_S)? 1 : 0
	cmpgaui	rB,	rA,	imm		rB ← (rA ≥ imm_U)? 1 : 0
	cmpltui	rB,	rA,	imm		rB ← (rA_U < imm_U)? 1 : 0
	cmpga	rC,	rA,	rB		rC ← (rA ≥ rB)? 1 : 0
	cmplt	rC,	rA,	rB		rC ← (rA < rB)? 1 : 0
	cmpna	rC,	rA,	rB		rC ← (rA ≠ rB)? 1 : 0
	cmpeq	rC,	rA,	rB		rC ← (rA = rB)? 1 : 0
	cmpgau	rC,	rA,	rB		rC ← (rA_U ≥ rB_U)? 1 : 0
	cmpltu	rC,	rA,	rB		rC ← (rA_U < rB_U)? 1 : 0
Shifts	sll	rC,	rA,	rB		rC ← rA << rB$_{4..0}$
	slli	rC,	rA,	imm		rC ← rA << imm$_{4..0}$
	srl	rC,	rA,	rB		rC ← rA_U >> rB$_{4..0}$
	srli	rC,	rA,	imm		rC ← rA_U >> imm$_{4..0}$
	sra	rC,	rA,	rB		rC ← rA_S >> rB$_{4..0}$
	srai	rC,	rA,	imm		rC ← rA_S >> imm$_{4..0}$
	rol	rC,	rA,	rB		rC ← rA *rol* rB$_{4..0}$
	ror	rC,	rA,	rB		rC ← rA *ror* rB$_{4..0}$
	roli	rC,	rA,	imm		rC ← rA *rol* imm$_{4..0}$
Memory	ldw	rB,	imm	(rA)	y	rB ← MEM[imm_S+rA]
	stw	rB,	imm	(rA)	y	MEM[imm_S+rA] ← rB
Branch	br	imm			y	PC ← PC+4+imm_S
	bge	rA,	rB,	imm		if(rA ≥ rB) PC ← PC+4+imm_S
	blt	rA,	rB,	imm		if(rA < rB) PC ← PC+4+imm_S
	bne	rA,	rB,	imm	y	if(rA ≠ rB) PC ← PC+4+imm_S
	beq	rA,	rB,	imm	y	if(rA = rB) PC ← PC+4+imm_S
	bgeu	rA,	rB,	imm		if(rA_U ≥ rB_U) PC ← PC+4+imm_S
	bltu	rA,	rB,	imm		if(rA_U < rB_U) PC ← PC+4+imm_S
Jump[2]	call	imm				PC ← imm << 2 ; retAdd←PC+4
	callr	rA				PC ← rA ; retAdd←PC+4
	ret					PC ← retAdd
	jmp	rA				PC ← rA
	jmpi	imm			y	PC ← imm << 2
System	IntEn	Int_I				Enable interrupt Int_I
	IntDs	Int_I				Disable interrupt Int_I

[1] imm=$IR_{15..0}$ unless otherwise noted, imm_S is signed, imm_U is unsigned
[2] for Jump instructions imm=$IR_{27..0}$

PROBLEM F2 – COMPUTER SYSTEMS

Digital Systems

Fibonacci sequences have many interesting properties and show up in unexpected situations. If you take the Fibonacci sequence and you compute the values, modulo-n, the resulting sequence shows peridicity. Note the following examples:

Series	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	...					
Series mod-3	0	1	1	2	0	2	2	1	**0**	**1**	**1**	**2**	**0**	**2**	**2**	**1**	0	1	1	2	0	2	2	1	0	1
Series mod-4	0	1	1	2	3	1	**0**	**1**	**1**	**2**	**3**	**1**	0	1	1	2	3	1	0	1	1	2	3	1	0	1
Series mod-5	0	1	1	2	3	0	3	3	1	4	0	4	4	3	2	0	2	2	4	1	**0**	**1**	**1**	**2**	**3**	**0**

Also note that Fibonacci numbers are defined as $F(n) = F(n-1) + F(n-2)$ where $F(0) = 0$ and $F(1) = 1$.

The period is called the Pisano period (note that Pisano is Fibonacci's surname) and is designated by $\pi(m)$ and the period for a given modulus m. From the table above, $\pi(3) = 8$, $\pi(4) = 6$, and $\pi(5) = 20$.

Designing a clocked sequential circuit with an asynchronous reset that calculates $\pi(m)$ given an input of m.

1. (1 point)
   Give an entity for this system.

2. (5 points)
   Provide a behavioral VHDL model that is consistent with your entity.

3. (4 points)
   Provide a State Machine Chart {SM Chart} (or Algorithmic State Machine Chart {ASM Chart}) suitable for register transfer level implementation. Fully define any registers that are implied by your SM Chart, including any signals necessary for their control.

PROBLEM F3 – COMPUTER SYSTEMS

Computer Architecture

1. Suppose the current program counter (PC) is set to 2000 0000_{hex}. Is it possible to use the jump (j) MIPS instruction to set the PC to the address as 2200 0000_{hex}? Why? (need to elaborate on how you get your answer.

2. If we have hit the power wall, we have to reduce the power consupmption, but still want to increase the performance of the computer in terms of CPU exeecution time for a program. How can we achive this with and withou a better cooling technology? Why?

PROBLEM F4 – COMPUTER SYSTEMS

Computer Algorithms

Given: a graph G=(V,E)
Output: a set of N partitions where the number of cuts are minimized

1. (2 points) Give an example of a graph with 10 nodes and 30 edges partitioned into four groups. Your partitions do not have to have a minimum number of cuts.
2. (6 points) Give an algorithm that given a graph G that finds a partition of N groups with a minumun number of cuts.
3. (2 points) Estimate the time complexity of your algorithm.

PROBLEM F5 – COMPUTER SYSTEMS

Data Structure

1.
A stack bStack contains the following items

7
8
-3
14
5
What is the output to the screen of the following code?

```
Int x;
While (!bStack.isEmpty()){
        bStack.pop(x);
        if (x>0&&!bStack.isEmpty())
                bStack.pop();
                cout <<x<<endl;
}
```

2.

Please provide pseudo code or diagram (explanations) for following questions

Given the input A (2, 1,0, 10 0, 9, 9, 10)
2.1 Construct a binary search tree according to the input A sequence.

2.2 Add a node, 5, into this binary search tree?

2.3 Delete a node, 0, from this binary search tree?

PROBLEM F6 – COMPUTER SYSTEMS

Logic Design

A circuit accepts a 4-bit (A, B, C and D) number such that:

F =1 if the number contains 3 consecutive 0's or 3 consecutive 1's and the **number is in the decimal range**, else F =0

F = d for numbers **outside** the decimal range. (d = don't care)

(a) (6 pts) Using K-map give the **minimal Sum-of-Product (SOP)** form of F.

AB / CD	00	01	11	10
00				
01				
11				
10				

(b) (4 pts) Implement the **minimized SOP of F** in part (a) using a 4-1 Mux.

PROBLEM G1 – CYBERSECURITY

1. Consider the 3-bit block cipher given in Table 1 below. Suppose the plaintext is 110101101.
    a) Initially assume that CBC (Cipher Block Chaining) is not used. What is the resulting ciphertext?
    b) Suppose James sniffs the ciphertext. Assuming he knows that a 3-bit block cipher without CBC is being employed (but doesn't know the specific cipher), what can she surmise?
    c) Now suppose that CBC is used with Initialization Vector, IV=111. What is the resulting ciphertext?

Input	Output
000	110
001	111
010	101
011	100
100	011
101	010
110	000
111	001

Table 1: A specific 3-bit block cipher

PROBLEM G2 – CYBERSECURITY

Cyber Defense Fundamentals

1. (10 pts) Describe how the RSA algorithm work? That is, how does Bob generate his public key, which is sent to Alice, and then how does Alice encrypt her message **m** using the public key, and eventually, how does Bob decrypt the received ciphertext?

PROBLEM G3 – CYBERSECURITY

Cyber Physical System Security

1. (5 pts) What are the two types of intrusion detection systems?

2. (5 pts) What is network address translation (NAT) and how does it work?

PROBLEM G4 – CYBERSECURITY

Problem 1

Alice wants to send a text message to Bob securely, over an insecure communication network. Alice's phone has a RSA public Key K_A and matching private key v_A; likewise, Bob's phone has K_B and matching private key v_B. Let's design a cryptographic protocol for doing this, assuming both know each other's public keys.

Here is what Alice's phone will do to send the text message m:

1. Alice's phone randomly picks a new AES session key k and computes c=RSA-Encrypt(K_B,k), c'=AES-CBC-Encrypt(k,m), and t=RSA-Sign(v_A,(c,c')).
2. Alice's phone sends (c,c',t) to Bob's phone.

And here is what Bob's cellphone will do, upon receiving (c,c',t):

1. Bob's phone checks that t is a valid RSA signature on (c,c') under public key K_A. If not, abort.
2. Bob's phone computes k'=RSA-Decrypt(v_B,c) and m'=AES-CBC-Decrypt(k',c')
3. Bob's phone informs Bob that Alice sent message m'

a) Does this protocol provide confidentiality of Alice's messages? Explain?

b) Does this protocol ensure authentication and data integrity for every text message Bob receives? Why or why not?

c) Suppose that Bob is Alice's stockbroker. Bob hooks up the output of this protocol to an automatic stock trading service, so if Alice sends a text message "Sell 100 shares MSFT" using the above protocol, then this trade will be immediately and automatically executed from Alice's' account. Suggest one reason why this might be a bad idea from a security point of view.

Problem 2: For the code given below, provide the expected output when the argv[1] to the *printf* function is passed with the following different values.

a. if argv[1] is passed "\x10\x01\x48\x08 %s"

b. if attacker exploits format string vulnerability to overwrite a pointer in the program, he will pass the following string to argv[1]. At what address does the attacker think the pointer is located? Give the address in hex.

c. What value is the attacker overwriting the pointer with? Give the value in hex

```
#include <stdio.h>
int main(int argc, char * argv[])
{
  printf("Your argument is:\n");
  // Does not specify a format string, allowing the user to supply one
  printf(argv[1]);
}
```

PROBLEM G5 – CYBERSECURITY

Security and Privacy of Embedded Systems

The sensors in certain embedded systems use communication protocols where data from various on-board sensors is read as a stream of bytes from a designated port or network socket. The code bellow illustrates one such scenario. The programmer expects to read at most 16 bytes of sensor data, storing them into the array **sensor_data**.

```
char sensor_data [16];
int secret-key;
void read_sensor_data () {
   int i  = 0;
        // more_data returns 1 if there is more data, and 0 otherwise
   while (more_data () {
      sensor_data [i] = get_next_byte ();
       i++;
    }
    return;
}
```

Suppose an attacker has control of the above stream, either through physical access to the sensors or over the network. Name two vulnerabilities that the attacker can compromise the system in other ways.