Midterm #2 of ECE 639, (CRN: 25576)
6–7pm, Thursday, November 17, 2022, BHEE224.

1. Enter your student ID number, and signature in the space provided on this page.
2. This is a closed book exam.
3. The instructor will hand out loose sheets of paper for the rough work.
4. Neither calculators nor help sheets are allowed.

Name:

Student ID:

As a Boiler Maker pursuing academic excellence, I pledge to be honest and true in all that I do. Accountable together — We are Purdue.

Signature: Date:

Question 1: [25%]

Consider an (n, k) binary cyclic code with the generator polynomial denoted by $g(x)$. Suppose $g(1) = 0$. Prove that the value of $\mathsf{weight}(\vec{c}_i)$ is even for any codeword $\vec{c}_i$, $i \in \{1, \cdots, 2^k\}$.

Hint 1: for two binary vectors $\vec{a}$ and $\vec{b}$. If both $\mathsf{weight}(\vec{a})$ and $\mathsf{weight}(\vec{b})$ are even, then $\mathsf{weight}(\vec{a} + \vec{b})$ is even. You can use this fact directly.

Hint 2: Given $g(x)$, it is useful to convert $g(x)$ to the generating matrix G.

Question 2: [25%] Consider a primitive binary polynomial $p(x)$ satisfying $\deg(p(x)) = l$. Define $g(x) = (x+1) \cdot p(x)$. Consider a length $n = 2^l - 1$ code $\mathbb{C}$ such that the codeword polynomial is $c(x) = m(x) \cdot g(x)$ where the message polynomial $m(x)$ satisfies $\deg(m(x)) \leq n - l - 2$.

Prove that $\mathbb{C}$ is cyclic.

Hint: for any two monic polynomials $a(x)$ and $b(x)$, we always have

$$a(x) \cdot b(x) = \Big(\mathsf{l.c.m.}(a(x), b(x))\Big) \cdot \Big(\mathsf{g.c.d.}(a(x), b(x))\Big) \tag{1}$$

where "l.c.m." stands for least common multiple and "g.c.d." stands for greatest common divider. For example,

$$(x+1) \cdot p(x) = \Big(\mathsf{l.c.m.}(x+1, p(x))\Big) \cdot \Big(\mathsf{g.c.d.}(x+1, p(x))\Big). \tag{2}$$

Question 3: [25%] In the lecture, we proved that a Reed-Muller code $\mathrm{RM}(r, m)$ must have $d_{\min} = 2^{m-r}$. The proof is quite complicated and relies on induction. It turns out that proving $d_{\min} \leq 2^{m-r}$ is very easy. Please write down a short proof why $d_{\min} \leq 2^{m-r}$.

Hint: It can be easily done by following the construction of the generating matrix G of the $\mathrm{RM}(r, m)$ code.

Question 4: [25%] Consider a finite field $\mathrm{GF}(2^m)$ with $m \geq 5$ and let β denote a primitive element of $\mathrm{GF}(2^m)$. We use $\Phi_i(x) \in \mathrm{GF}(2)[x]$ to denote the *minimal polynomial* of element β^i. That is, $\Phi_i(x)$ has the roots β^i, $(\beta^i)^2$, $(\beta^i)^{2^2}$, $\cdots$, $(\beta^i)^{2^l}$ where l is the degree of $\Phi_i(x)$.

1. [10%] Prove that $\Phi_4(x) = \Phi_1(x)$;
2. [10%] Prove that $\Phi_6(x) = \Phi_3(x)$;
3. [5%] Prove that for any even integer $j \geq 2$, we can find an odd integer $1 \leq i < j$ satisfying $\Phi_j(x) = \Phi_i(x)$. Hint: as can be seen, this sub-question is a generalization of the previous two sub-questions.