## ECE/MATH 641: HOMEWORK 4, DUE NOV 17.

Please solve the following problems.

1. Let $C$ be a binary linear code such that $C \subseteq C^\perp$ (such a code is called self-orthogonal). Prove that every codeword of $C$ has even weight. If every row of the generator matrix is of weight divisible by 4, show that every codeword of $C$ is of weight divisible by 4. Is the last claim necessarily true if $C$ is not self-orthogonal?

2. The polynomial $x^{15} - 1$ factors over $\mathbf{F}_2$ as follows:

$$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Let $C$ be the $[15, k, d]$ binary cyclic code of length 15 generated by $g(x) = (x+1)(x^4+x+1)$.

(a) What are $k$ and the designed distance? What about the true minimum distance $d$?

(b) Is $x^{14} + x^{12} + x^8 + x^4 + x + 1$ a codeword in $C$?

(c) List all $[n = 15; k = 8]$ binary cyclic codes and their dual codes. For each code, just give its generator polynomial and check polynomial.

(d) What is the total number of binary cyclic codes of length 15?

3. Let $\Phi$ be a family of $[n, k]$ linear codes over $\mathbf{F}_q$ such that every vector of length $n$ is contained in the same number of codes from the family.

(a) Show that if

$$\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \; < \; \frac{q^n - 1}{q^k - 1},$$

then $\Phi$ contains a code with minimum distance $d$.

(b) Let $q = 2$. Conclude that for $n \to \infty$, $\Phi$ contains codes that meet the asymptotic Gilbert-Varshamov bound.

4. Does there exist a binary linear $[38, 9, 19]$ code? Explain why or why not.