Preliminary Exam
Coding Theory

March 16, 1994

1) Show that any Reed-Solomon code satisfies the Singleton bound $d \leq n+1-k$ with equality. Why must the dual of a Reed-Solomon code also be a Reed-Solomon code?

2) Perfect e-error-correcting codes are those for which *every* received word r is at most e errors away from exactly one codeword c(r). [Examples are Hamming codes for e=1, the binary Golay code (with length 23) for e=3, and the ternary Golay code (with length 11) for e=2.] How many codewords of minimum weight $d=2e+1$ are there in a perfect e-error-correcting code $\mathcal{C}$? [Hint: Consider the received words of weight e+1.]

3) Consider the Reed-Solomon code over $GF(8)=GF(2)[\delta]/(1+\delta+\delta^3)$ with generator polynomial

$$g(x)=(\delta^1+x)(\delta^2+x)(\delta^3+x)(\delta^4+x)=\delta^3+\delta^1x+x^2+\delta^3x^3+x^4.$$

a) What is the generator matrix implicit in polynomial encoding?

b) What is the generator matrix implicit in functional encoding?

4) An idempotent e(x) for a code $\mathcal{C}$ must satisfy $e(x)\in\mathcal{C}$, $e^2(x)=e(x)$, and $e(x)c(x)=c(x)$ for $c(x)\in\mathcal{C}$. [The binary linear, cyclic code $\mathcal{C}$ of length 7 with generator polynomial $g(x)=1+x+x^3$ has at least the idempotent $e(x)=x+x^2+x^4$.]

a) Show that any binary linear, cyclic code of odd wordlength has an idempotent. [Hint: Consider the Euclidean algorithm.]

b) Is there always an idempotent generator?

5) The Berlekamp-Massey algorithm applied to a polynomial a(x) recursively produces polynomials $p_t(x)$, of degree at most t, such that $r_t(x)=p_t(x)a(x) \pmod{x^{2t+1}}$ also has degree at most t. How does this give a solution to Newton's identities

$$s_{j+e}+\sigma_1 s_{j+e-1}+\cdots+\sigma_e s_j=0,\ \ell+1\leq j\leq \ell+e,$$

for finding the symmetric functions σ_i $1\leq i\leq e$, (coefficients of the error-locator polynomial $\sigma(x)$) in terms of the power sums (syndromes) s_j, $\ell+1\leq j\leq \ell+2e$, used in decoding BCH codes? [That is, what are a(x) and $p_t(x)$ and why does a particular $p_t(x)$ solve Newton's identities?]