MATH447/747 ASSIGNMENT 3

FALL 2012

The following questions are optional questions. They do not need to be handed in and will not be graded if they are handed in

- Vanstone and van Oorschot section 3.9 # 13, 21
- Vanstone and van Oorschot section 3.9 # 26. What if the code must be linear? What if it is not necessarily linear?

The following questions are to be handed in. They are due **Friday September 28** in class.

(1) Let $x_1, x_2, \ldots, x_n$ be commuting indeterminants. Let

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}$$

(a) Show that $x_i - x_j$ divides $\det V$ by considering what happens if we set $x_i = x_j$ in V.

(b) Show that $\det V = \prod_{1 \le i < j \le n} (x_j - x_i)$

(c) Let a be a primitive element of $\mathbb{F}_p$ with p prime. Let

$$H = \begin{bmatrix} 1 & a & a^2 & \cdots & a^{p-2} \\ 1 & a^2 & a^4 & \cdots & a^{2(p-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a^k & a^{2k} & \cdots & a^{k(p-2)}) \end{bmatrix}$$

with $k < p - 2$ be the parity check matrix for a linear code C. What is the distance of C?

(2) Vanstone and van Oorschot section 3.9 # 7. You may use a computer, but if you do then please submit the sequence of commands you use or the source for the program you write.

(3) Vanstone and van Oorschot section 3.9 # 36, 69, 70