Solutions to mid term exam, December, 3 2015

Exercice 1. 1. By definition of the covering radius, for every $y \in \mathbb{F}_q^n$, there exists $c \in C$ such that $d_H(c, y) \leqslant \rho$. Thus, $y \in \mathbf{B}_H(c, \rho)$. Conseqeuntly,

$$\bigcup_{c \in C} \mathbf{B}_H(c, \rho) = \mathbb{F}_q^n.$$

2. The Hamming code is perfect and has minimum distance 3. Hence, its covering radius is 1.
3. From Question 1, we have
$$\forall s \in \mathbb{N},\ q^{k_s} \mathrm{Vol}_q(\rho_s, n_s) \geqslant q^{n_s}.$$
Moreover,
$$\mathrm{Vol}_q(\rho_s, n_s) \leqslant q^{n_s H_q(\frac{\rho_s}{n_s})}.$$
Therefore, after applying $\log_q$, which is an increasing function, we get :
$$\frac{k_s}{n_s} + H_q(\frac{\rho_s}{n_s}) \geqslant 1$$
and, by continuity of H_q, when s tends to infinity, we get
$$H_q(P) \geqslant 1 - R.$$
4. After a possible permutation of the coordinates, one can obtain by Gaussian elimination a generator matrix for C in *systematic form*. That is a generator matrix of the form
$$\mathbf{G} = \begin{pmatrix} \mathrm{I}_k & | & (*) \end{pmatrix}$$
where I_k denotes the $k \times k$ identity matrix. Now, let $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$. Then, $c_y := (y_1, \ldots, y_k)\mathbf{G}$ is in C and the words, y, c_y coincide on the k first positions. Therefore, $d_H(y, c_y) \leqslant n-k$. Thus $\rho \leqslant n-k$.
5. Let $g \in \mathbb{F}_q[X]_{<k}$ and $c_g \in \mathbf{RS}_k(\alpha)$ the word $c_g := (g(\alpha_1), \ldots, g(\alpha_n))$ such that
$$d_H(y_f, c_g) = d_H(y_f, \mathbf{RS}_k(\alpha)).$$
Then $w_H(y_f - c_g) = w_H(((f-g)(\alpha_1), \ldots, (f-g)(\alpha_n)))$. Since $\deg(f-g) = k$, the polynomial $f-g$ has at most k roots and hence,
$$w_H(y_f - c_g) = d_H(y_f, \mathbf{RS}_k(\alpha)) \geqslant n-k.$$
Using the previous question, we see than the above inequality should be an equality.
6. We proved in the previous question that words obtained by evaluation of polynomials of degree k are at distance $n-k$ from the code. Since the covering radius is at most $n-k$. The covering radius of an RS code is $n-k$ and the words associated to polynomials of degree k are at distance $n-k$ from the code.

7. Let $f \in \mathbb{F}_q[X]_{<k}$.

$$\begin{aligned} d_H((f(\alpha_1), \dots, f(\alpha_n)), (\alpha_1^{-1}, \dots, \alpha_n^{-1})) &= w_H((f(\alpha_1) - \alpha_1^{-1}, \dots, f(\alpha_n) - \alpha_n^{-1})) \\ &= w_H((\alpha_1 f(\alpha_1) - 1, \dots, \alpha_n f(\alpha_n) - 1)) \end{aligned}$$

and the last quantity is bounded below by n minus the number of roots of the polynomial $Xf(X) - 1$. Since this polynomial has degree at most k, it has at most k roots. Hence,

$$d_H((f(\alpha_1), \dots, f(\alpha_n)), (\alpha_1^{-1}, \dots, \alpha_n^{-1})) \geqslant n - k$$

and from Question 4, the above inequality is an equality.

Exercice 2. 1.

$$\pi_{\mathbf{c}}\pi_{\mathbf{c}'} = \prod_{i=1}^{n} (X - x_i)^{a_i}$$

where

$$a_i = \begin{cases} 2 & \text{if} \quad c_i = c'_i = 1 \\ 1 & \text{if} \quad \text{only one of the } c'_i s \text{ equals } 1 \\ 0 & \text{else} \end{cases}$$

It is easy to observe that $\pi_{\mathbf{c}+\mathbf{c}'}\pi_{\mathbf{c}\cap\mathbf{c}'}$ has the same factorization.

2. $\pi_{\mathbf{c}}$ is split with simple roots among $x_1, \dots, x_n$ while g does not vanish at these elements. Thus g and $\pi_{\mathbf{c}}$ have no common irreducible factor.
3. One proves first that
$$(\pi_{\mathbf{c}+\mathbf{c}'}\pi^2_{\mathbf{c}\cap\mathbf{c}'})' = \pi^2_{\mathbf{c}\cap\mathbf{c}'}\pi'_{\mathbf{c}+\mathbf{c}'}.$$
Indeed, since we are in characteristic 2, the derivative of a square is 0. Next, we also have
$$(\pi_{\mathbf{c}+\mathbf{c}'}\pi^2_{\mathbf{c}\cap\mathbf{c}'})' = (\pi_{\mathbf{c}}\pi_{\mathbf{c}'})' = \pi'_{\mathbf{c}}\pi_{\mathbf{c}'} + \pi_{\mathbf{c}}\pi'_{\mathbf{c}'}.$$
Therefore, if $\mathbf{c}, \mathbf{c}' \in \Gamma(\mathbf{x}, g)$, then g divides $\pi'_{\mathbf{c}}$ and $\pi'_{\mathbf{c}'}$. Thus, it divides $\pi'_{\mathbf{c}}\pi_{\mathbf{c}'} + \pi_{\mathbf{c}}\pi'_{\mathbf{c}'}$ which equals $\pi^2_{\mathbf{c}\cap\mathbf{c}'}\pi'_{\mathbf{c}+\mathbf{c}'}$. Finally, from the previous question, g is prime to $\pi_{\mathbf{c}\cap\mathbf{c}'}$ and hence it divides $\pi'_{\mathbf{c}+\mathbf{c}'}$. Therefore $\mathbf{c} + \mathbf{c}' \in \Gamma(\mathbf{x}, g)$
4. Let $\mathbf{c} \in \Gamma(\mathbf{x}, g) \setminus \{0\}$. Then $g|\pi'_{\mathbf{c}}$ and hence either $\deg \pi'_{\mathbf{c}} \geqslant \deg g$ or $\pi'_{\mathbf{c}} = 0$. But $\pi_{\mathbf{c}}$ is squarefree, while the polynomials with zero derivative in $\mathbb{F}_{2^m}[X]$ are the squares.
Thus, $\deg \pi'_{\mathbf{c}} \geqslant \deg g$ and $\deg \pi_{\mathbf{c}} \geqslant \deg g + 1$. To conclude, it suffices to notice that $\deg \pi_{\mathbf{c}} = w_H(\mathbf{c})$.
5. Write $f = f_0 + f_1 X + \cdots + f_n X^n$. Then, $f' = f_1 + f_3 X^2 + f_5 X^4 + \cdots$ In particular f' has only terms of even degree. Then, since the Frobenius map is surjective in $\mathbb{F}_{2^m}$, we get
$$f' = (f_1^{1/2} + f_3^{1/2} X + f_5^{1/2} X^2 + \cdots)^2.$$
where $f_i^{1/2}$ denotes the inverse image of f_i by the Frobenius map.
6. Inclusion $\supseteq$ is obvious, indeed, if $g^2|\pi'_{\mathbf{c}}$, then $g|\pi'_{\mathbf{c}}$.
Conversely, if $g|\pi'_{\mathbf{c}}$, then, since g is squarefree and, from the previous question, $\pi'_{\mathbf{c}}$ is a square, then $g^2|\pi'_{\mathbf{c}}$.
7.
$$\begin{aligned} \psi(fg) &= \frac{f'g + fg'}{fg} \\ &= \frac{f'}{f} + \frac{g'}{g}. \end{aligned}$$

8. First notice that ψ sends squares onto 0. Hence, thanks to the previous question, for all $\mathbf{c}, \mathbf{c}' \in \mathbb{F}_2^n$, we have
$$\psi(\pi_{\mathbf{c}+\mathbf{c}'}) = \psi(\pi_{\mathbf{c}+\mathbf{c}'}\pi^2_{\mathbf{c}\cap\mathbf{c}'}).$$
Next, form question 1, we get
$$h(\mathbf{c}+\mathbf{c}') = \psi(\pi_{\mathbf{c}+\mathbf{c}'}) = \psi(\pi_{\mathbf{c}}\pi_{\mathbf{c}'}) = h(\mathbf{c}) + h(\mathbf{c}').$$
This proves the $\mathbb{F}_2$–linearity of h. Now, to prove injectivity, notice that $h(\mathbf{a}) = 0$ entails that $\pi'_{\mathbf{a}} = 0$ and hence that $\pi_{\mathbf{a}}$ is a square which is impossible since this polynomial is squarefree unless $\mathbf{a} = 0$.

9. The dimension $\mathbb{F}_{2^m}$–dimension of E is n and its $\mathbb{F}_2$–dimension is mn. The $\mathbb{F}_{2^m}$–dimension of E_g is $n - \deg g$ and its $\mathbb{F}_2$–dimension is $m(n - \deg g)$.

10. Let $\mathbf{a} \in \mathbb{F}_2^n$. Then, $\pi_{\mathbf{a}} | \prod_{i=1}^n (X - x_i)$. and $\pi'_{\mathbf{a}}$ has degree at most $n-1$. Thus, $h(\mathbf{a}) \in E$.

11. $\Gamma(\mathbf{x}, g)$ is the kernel of the composition of the maps $h : \mathbb{F}_2^n \to E$ and the canonical quotient projection $E \to E/E_g$. By the rank nullity theorem, this kernel has dimension at least $n - \dim_{\mathbb{F}_2} E/E_g$. We conclude using question 9.