Mathematics 601
Homework Assignment #3

Work any four of the following problems. These are due on Monday 3 December.

1. Let $C$ be a code over $\mathbb{F}_q$ described as the nullspace of a matrix $H$. Let $n$ be a positive integer and let $C'$ be the nullspace of $H$ viewed as a code over $\mathbb{F}_q^n$. Prove that $C = C'|_{\mathbb{F}_q}$. Also, show that the distance of $C$ is equal to the distance of $C'$.

2. Let $H$ be a parity check matrix for a code $C$. If $\{v_1, \ldots, v_k\}$ is a basis for the nullspace of $H$, prove that the matrix $G$ whose rows are $v_1, \ldots, v_k$ is a generator matrix for $C$.

Likewise, if you start with a generator matrix $G$, and if $\{w_1, \ldots, w_{n-k}\}$ form a basis for the nullspace of $G$, show that the matrix $H$ whose rows are $w_1, \ldots, w_{n-k}$ is a parity check matrix for $H$.

(The first fact was used to write for the procedure GeneratorMatrix in the worksheet Codes.mws).

3. Let $f = x^2 - xy + y^2 + 1$, and let $F = \mathbb{F}_3(\overline{x}, \overline{y})$ be the function field of the affine curve $Z(f)$ over $\mathbb{F}_3$.

   (a) Show that $f$ is irreducible in $\mathbb{F}_3[x, y]$ (so the function field of $f$ does exist).
   
   (b) Show that $f$ factors in $\mathbb{F}_9[x, y]$. Recall that $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, where $\alpha^2 = -1$.
   
   (c) Show that the exact field of constants of $F/\mathbb{F}_3$ is $\mathbb{F}_9$. (Hint: show that $F = \mathbb{F}_9(\overline{x})$).

4. Let $r$ be a positive integer, and consider the Galois group $G = \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. For $\sigma \in G$, let $\sigma$ act on the vector space $\mathbb{F}_{q^r}^n$ of $n$-tuples over $\mathbb{F}_{q^r}$ by $\sigma((a_1, \ldots, a_n)) = ((\sigma(a_1)), \ldots, (\sigma(a_n)))$.

   (a) Show that $\sigma(v + w) = \sigma(v) + \sigma(w)$ and $\sigma(\alpha v) = \sigma(\alpha)\sigma(v)$ for any $v, w \in \mathbb{F}_{q^r}^n$ and $\alpha \in \mathbb{F}_{q^r}$.
   
   (b) Let $C$ be a code of length $n$ over $\mathbb{F}_{q^r}$, and suppose that $\sigma(C) = C$ for all $\sigma \in G$.

   Show that $C|_{\mathbb{F}_q} = \{v \in C : \sigma(v) = v \text{ for all } \sigma \in G\}$.
   
   (c) If $\dim_{\mathbb{F}_q}(C|_{\mathbb{F}_q}) = \dim_{\mathbb{F}_{q^r}}(C)$, show that $\sigma(C) = C$ for all $\sigma \in G$.
   
   (d) Extra Credit: if $\sigma(C) = C$ for all $\sigma \in C$, show that $\dim_{\mathbb{F}_q}(C|_{\mathbb{F}_q}) = \dim_{\mathbb{F}_{q^r}}(C)$.

1
5. Let $C$ be the rational Goppa code $C_L(D,G)$ over $\mathbb{F}_8$, where $G = 4P_\infty$ and $D = P_{\alpha_1} + \cdots + P_{\alpha_8}$, where $P_\alpha$ is the place corresponding to the point $(\alpha : 0 : 1)$. You may view the function field as $\mathbb{F}_8(x)$, the function field of the curve $y = 0$. The divisor $D$ is then the sum of all the rational points other than $P_\infty$. Write out a generator matrix and verify that the distance of this code is 5 with the procedure DistanceG in Codes.mws.

6. Let $C$ be the code $C_L(D,G)$ over $\mathbb{F}_{64}$ associated to the function field of the Hermitian curve with equation $y^8z + yz^8 = x^9$, where $G = 17P_\infty$ and where $D$ is the sum of the first twenty points that the procedure Ppoints.mws finds. You need to find a sixth degree polynomial to represent $\mathbb{F}_{64}$ (you may use the procedure DefineP in the file MakeGenerator.mws to do this, although using this procedure is not necessary). Determine the dimension of $L(G)$, and write down a generator matrix for $C$. You will find the procedure MakeGeneratorMatrix in MakeGenerator.mws convenient in writing out a generator matrix, and ChangeMatrix may be helpful to simplify the writing of the matrix.

7. Let $X$ be the curve $y^2z^2 = x^4 + x^2z^2 + 2z^4$ over $\mathbb{F}_3$. With the help of the procedure Ppoints in POINTS.mws, find the number of points of $X$ of degree 1, degree 2, and degree 4. Pick a point of degree 2 and one of degree 4 and find all the conjugates of the given point. The conjugates of a point $P$ are the points $\{\sigma(P) : \sigma \in \text{Gal}(K/\mathbb{F}_3)\}$ if the coordinates of $P$ lie in the field $K$.

(Note: $X$ is an example of a curve with two points at infinity, although this fact is not relevant for the problem.)

8. Let $X$ be the elliptic curve $y^2z = x^3 - xz^2 - z^3$ over $\mathbb{F}_3$. With the help of Points.mws, determine the number of places (not points!) of degree 2 and degree 3 of the function field of $X$.

9. Let $X$ be the Hermitian curve $y^8z + yz^8 = x^9$ over $\mathbb{F}_{64}$. Calculate the divisor of the function $(x + y)/z$.

(Hint: find all the $\mathbb{F}_{64}$-points of the curve with Ppoints in the worksheet POINTS.mws. which will enter a list called Points into memory. (Since there are 513 such points, it will take Maple a little while to do this.) Search the list to find those with $y = x$. Since the list will be long, use the Maple code $\text{for i from 1 to 513 do if Points[i][1]=Points[i][2] then print(Points[i]) fi end do}$ (all one line). You should ask yourself why only knowing the $\mathbb{F}_{64}$-rational points of the curve is enough to find the divisor of $(x + y)/z$.

10. Let $X$ be the elliptic curve $y^2z = x^3 - z^3$ over $\mathbb{F}_5$. Calculate the divisor of the function $(2x + y)/z$. 
