Math 342, Spring Term 2009
Pre-Final Sheet

April 13, 2009

The exam has been scheduled for Thursday, April 16^{th} between 15:30-18:00 at Room 100 of the Math Building.

Material

The material for the exam consists of all the material covered in the lectures up to and including Friday, April 3^{rd}, as well as Problem Sets 1 through 12.

Structure

The exam will consist of several problems. Problems can be calculational (only the steps of the calculation are required), theoretical (prove that something holds) or factual (state a Definition, Theorem, etc). The sample and actual midterm exams present

Sample paper

1. Let F be a field, V a vector space over F.
   - (a) State what it means for a subset $W \subset V$ to be a *subspace*.
   - (b) For $V = F^4$, show that $W = \{(x, y, z, w) \in V \mid x + y = z + w\}$ is a subspace.
   - (c) Assume that $F = \mathbb{F}_q$ is the field with q elements. What is $\#V$?
   - (d) Let $U = \{(x, y, 0, 0) \in V\}$. What is $\#U$? Show that $\#U | \#V$
   - (e) Explain why your answer to (d) is a special case of Lagrange's Theorem.
2. Find all solutions to the following systems of equations:

(a) $4x \equiv 5\,(12)$, where $x \in \mathbb{Z}$.

(b) $\begin{cases} [5]_{10}x + [3]_{10}y \equiv [2]_{10} \\ [4]_{10}x + y = [0]_{10} \end{cases}$, where $x, y \in \mathbb{Z}/10\mathbb{Z}$

(c) $x^2 = [2]_3$, $x \in \mathbb{Z}/3\mathbb{Z}$.

3. PS1 problem 4

4. PS3 problem 9

5. PS10 problem 5.

6. Let $H = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 1 \end{pmatrix} \in M_{2\times 4}(\mathbb{F}_3)$ and let $C \subset \mathbb{F}_3^4$ be the code defined by $C = \{\underline{v} \mid H\underline{v} = \underline{0}\}$.

   (a) For any $x, y \in \mathbb{F}_3$ show that there is are unique $z, w \in \mathbb{F}_3$ so that $\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} \in C$.

   (b) Write a *generating matrix* for this code. This matrix will represent the encoding function $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$ where z, w are as in part (a).

   (c) What is the *weight* of this code?

   (d) Can this code correct errors?

7. (RS codes)

   (a) Given integers $k \leq n$, a finite field F, and a subset $X \subset F$ of size n, define the *Reed-Solomon code of dimension k in F^n* given by evaluation at X.

   (b) Show that the code you defined has weight at least $n - k + 1$.

   (c) Let $F = \mathbb{F}_7$, $k = 2$, $n = 5$. You have received the vector $\underline{v}' = (2, 6, 0, 0, 4) \in \mathbb{F}_7^5$ which (up to transmission errors) represents the values of a linear polynomial at the points $X = \{1, 2, 3, 4, 5\} \in \mathbb{F}_7$. Which linear polynoimal is the maximum likelihood decoding of this transmission? Prove your claim.

8. The group of rigid symmetries of the square is a subgroup $D_4 \subset S_4$ of order 8. In contains a cyclic subgroup of order 4 – the rotations – which we will denote C_4. D_4 also contains the reflection by a diagonal, which we denote π. Using Lagrange's Theorem show that every symmetry of the square is either of the form ρ or $\pi\rho$ for some rotation $\rho \in C_4$.

Sample solutions

1. Let F be a field, V a vector space over F.

   (a) A subset $W \subset V$ is a subspace if it is non-empty and is closed under addition and under multiplication by scalars.

   (b) If $x = y = z = w = 0$ then clearly $x + y = z + w$ so $\underline{0} \in W$. Also, if $(x, y, z, w), (x', y', z', w') \in W$ and $\alpha \in F$ then the associtativity and commutativity of addition in F show that $(x + x') + (y + y') = (x+y)+(x'+y')$ while $(z+z')+(w+w') = (z+w)+(z'+w')$. Since $(x + y) = (z + w)$ and $(x' + y') = (z' + w')$ it follows that $(x + x') + (y+y') = (z+z')+(w+w')$, that is that $(x, y, z, w)+(x', y', z', w') = (x+x', y+y', z+z', w+w') \in W$. We also have $\alpha(x+y) = \alpha(z+w)$. By the distributive law in F we have $\alpha x + \alpha y = \alpha z + \alpha w$, that is that $\alpha(x, y, z, w) = (\alpha x, \alpha y, \alpha z, \alpha w) \in W$.

   (c) V is the space of 4-tuples of elements drawn from a set of size q, so $\#V = q^4$.

   (d) Similarly, $\#U = q^2$ which divides its square q^4.

   (e) $U \subset V$ is a subspace. In particular, it is a subset of V containing the zero vector and closed under addition. Thinking only of the additive group $(V, \underline{0}, +)$, U is a subgroup. Its order must divide that of V by Lagrange's Theorem.

2. Find all solutions to the following systems of equations:

   (a) Since $4x$ is even for all $x \in \mathbb{Z}$, $4x - 5$ is always odd and in particular not divisible by 12. It follows that there are no solutions to the equation.

   (b) Let $x, y \in \mathbb{Z}/10\mathbb{Z}$ be solutions to the equation. Multiplying the second equation by $[3]_{10}$ and subtracting the two equations shows $[3]_{10}x = [2]_{10}$. Since $7 \cdot 3 \equiv 1\,(10)$ this implies $x = [7]_{10}[2]_{10} = [4]_{10}$. The second equation then shows $[6]_{10} + y = [0]_{10}$, that is $y = [4]_{10}$ as well. We also have $5\cdot 4+3\cdot 4 = 32 \equiv 2\,(10)$. Thus $x = [4]_{10}$, $y = [4]_{10}$ is the unique solution to the system of equations.

   (c) We have $[0]_3^2 = [0 \cdot 0]_3 = [0]_3$, $[1]_3^2 = [1 \cdot 1]_3 = [1]_3$, $[2]_3^2 = [2 \cdot 2]_3 = [4]_3 = [1]_3$. Since $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$ the equation has no solutions.

3. PS1 problem 4.

4. PS3 problem 9.

5. PS10 problem 5.

6. Let $H = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 1 \end{pmatrix} \in M_{2\times 4}(\mathbb{F}_3)$ and let $C \subset \mathbb{F}_3^4$ be the code defined by $C = \{\underline{v} \mid H\underline{v} = \underline{0}\}$.

(a) We first show that if z, w exist they are unique. For this let $x, y, zw \in \mathbb{F}_3$ be such that $\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} \in C$. Then $x+y+2z = 0$ and $2y+z+w = 0$. Adding z to the first equation, $y+2z$ to the second, we find: $z = x+y$, $w = y+2z$, and both equatios imply $w = y+2(x+y) = 2x$, so that both z, w and uniquely determined by x, y. Conversely, given x, y setting $z = x+y$ and $w = 2x$ we have $x+y+2z = x+y+2(x+y) = 3(x+y) = 0$ and $2y+z+w = 2y+x+y+2x = 3(x+y) = 0$.

(b) $G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 2 & 0 \end{pmatrix}$.

(c) Since $G\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \in C$, the code has weight at most two. Conversely, let $\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} \in C$. If $x \neq 0$ then $w = 2x$ does not vanish as well (it is the product of two non-zero elements of a field) and the codeword has weight at least 2. If $x = 0$ but $y \neq 0$ then $z = y \neq 0$ and the codeword has weight two. If $x = y = 0$ then $z = w = 0$ as well and the codeword vanishes.

(d) Since the weight is two, the code is not guaranteed to correct even all 1-bit errors. For example, if we recieve the trasmission $\underline{v}' = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}$ it is equally consistent that the sender tramitted $\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 2 \\ 2 \\ 0 \end{pmatrix}$.

7. (RS codes)

(a) Say $X = \{x_i\}_{i=1}^n$ with the $x_i \in F$ distinct. The Reed-Solomon code is the set of n-tuples $\underline{v} \in F^n$ for which there exists $\underline{a} \in F^k$ such that for all $1 \leq i \leq n$, $v_i = \sum_{j=0}^{k-1} a_j x_i^j$, where we labelled the co-ordinates of $\underline{a}$ from 0 to $k-1$ instead of the usual 1 to k.

(b) Assume that there exists a non-zero $\underline{v} \in C_{\mathrm{RS}}$ of weight at most $n-k$, and say $\underline{v}$ is obtained by evaluating the polynomial $p(x) = \sum_{j=0}^{k-1} a_j x^j$ at the points of X. Since p takes non-zero values at no more than $n-k$

of the points of X, and hence vanishes in at least k distinct points of F. Thus p is a polynomial of degree at most $k-1$ with at least k distinct roots. We showed in class that the only such polynomial is the zero polynomial, at which point $p(x_i)=0$ for all i, so $\underline{v}=\underline{0}$ – a contradiction.

(c) We try the polynomial $\ell(x) = 4(x-1)+2 = 4x+5$, chosen so that $\ell(1)=2$, $\ell(2)=6$. It also has $\ell(3)=3$, $\ell(4)=0$, $l(5)=4$, so $\underline{v}=(2,6,3,0,4)$ is a codeword. We claim that it is the closest codeword to $\underline{v}'$. For this let $\underline{u}$ be any other codeword. We saw in part (b) that the weight of the code is at least $5-3+1=3$, so by the triangle inequality we have:

$$d_{\mathrm{H}}\left(\underline{u},\underline{v}'\right) + d_{\mathrm{H}}\left(\underline{v}',\underline{v}\right) \geq d_{\mathrm{H}}\left(\underline{u},\underline{v}\right) \geq 3\,.$$

Since $d_{\mathrm{H}}\left(\underline{v}',\underline{v}\right)=1$ this means

$$d_{\mathrm{H}}\left(\underline{u},\underline{v}'\right) \geq 2 > d_{\mathrm{H}}\left(\underline{v},\underline{v}'\right)\,.$$

8. In the space of equivalence classes of the relation $x \equiv_L y\,(C_4)$ (that is the space D_4/C_4 of left-C_4-cosets in D_4) consider the equivalence classes of the two elements $\mathrm{id},\pi \in D_4$. The two elements are not equivalent ($\mathrm{id}^{-1}\cdot\pi = \pi \notin C_4$). $x \in D_4$ is equivalent to id iff $x^{-1}\mathrm{id} \in C_4$, that is if $x \in C_4$. Also, $x \equiv_L \pi\,(C_4)$ iff $\pi^{-1}x \in C_4$. If we call this element ρ then $\pi^{-1}x=\rho$, and multiplying by π on the left we have $x=\pi\rho$ as claimed. It remains to show that every x belongs to one of the two equivalence classes. For this we use Lagrange's Theorem, according to which the number of equivalence classes is the ratio $\#D_4/\#C_4 = 8/4 = 2$.