Math 350
Spring, 2000

HOMEWORK #8

Do 50 points of the following problems (due 4/4/00).

25 pts. **1** Use the decoding scheme described by Jenny Key to decode the codeword 122011022 (show all work). You should use the definition of the code she gave in class.

The dot products with the 12 lines are 2; 0; 0; 1; 1; 0; 1; 1; 0; 1; 0; 1. From the description in class, position 0 uses lines l_2, l_5, l_9, and l_{10}, and those have dot products 0; 1; 0; 1: the error is not in position 0. Choosing the lines for each position, we get position 1 with 2; 1; 1; 1 (an error of 1 by majority vote in this position, so we will subtract 1 from the received word): position 2 with 2; 0; 0; 0 (no error): position 3 with 0; 0; 1; 1 (no error): position 4 with 2; 1; 1; 1 (an error of 1 by majority vote in this position, so we will subtract 1 from the received word): position 5 with 0; 0; 1; 1 (no error): position 6 with 0; 1; 0; 1 (no error): position 7 with 0; 1; 1; 0 (no error): and position 8 with 0; 1; 1; 0 (no error). Thus, we correct 122011022 by subtracting 010010000 to get the corrected 112001022. Note that this word is $l_{10} - l_{11}$.

⋆ 50 pts. **2** Describe how you would use the affine plane over $GF(p)$ to the general majority logic decoding algorithm similar to Jenny Key's description. What properties of the affine plane are useful here?

If we take any affine plane, and form the incidence matrix for the lines of the affine plane, we have the property that any pair of lines will intersect in a unique point. That point will be one of the positions of the code, so if we take all of the lines that have a 1 in position k, the rows for those lines will have the property that every other position has exactly one 1 in a column (if there were two, then two of the lines would meet in 2 positions. If there weren't any, then there would be a pair of points that did not determine a line). Since each point is on exactly $p+1$ lines (from work we did earlier on affine planes), we will have $p+1$ votes in each position. If the code is the orthogonal to the incidence matrix for the affine plane, then we should be able to correct up to $\frac{p+1}{2}$ errors in any positions (this code is over Z_p). This is true because if an error has been made in position i, then there are $\frac{p-1}{2}$ errors to spread across other positions. This will affect at most $\frac{p-1}{2}$ of the "votes", so the $\frac{p+3}{2}$ other "votes" will give the correct magnitude of the error in that position. If there is not an error in position i, then at most $\frac{p+1}{2}$ of the "votes" will be nonzero, leaving at least $\frac{p+1}{2}$ votes for 0. Any time there are that many zeros, we assume that there was not an error in that position. Thus, this allows us to correct at least $\frac{p+1}{2}$ errors in any position.

25 pts. **3** Let $1+x+x^4$ generate the binary Hamming code of length 15. Use the decoding algorithm discussed in class to decode $x+x^3+x^5+x^7+x^9+x^{11}$.

If $w(x) = x+x^3+x^5+x^7+x^9+x^{11}$, then $s(x) = 1+x$. This has weight 2, so we need to check the $s_i(x)$: $s_0(x) = x+1 (= x^4)$; $s_1(x) = x^2+x (= x^5)$; $\ldots$; $s_i(x) = \cdots (= x^{4+i})$; $\ldots$. Since $x^{15} = 1$ in this case, we get that $s_{11}(x) = 1$, so $e(x) = x^{15-11}s_{11}(x) = x^4$. Thus, the decoded word is $x+x^3+x^4+x^5+x^7+x^9+x^{11} = (x+x^2+x^4+x^5+x^7)(1+x+x^4)$.

25 pts. **4** Use the MacWilliams identities to find the weight enumerator for the orthogonal code to the first order Reed Muller code of length 16 (which has 30 codewords of weight 8, 1 codeword of weight 16, and 1 codeword of weight 0).

$W_C(z) = 1 + 30z^8 + z^{16}$: by the MacWilliams identities, $W_{C^\perp} = \frac{1}{2^5}(1+z)^{16}(1+30\frac{(1-z)^8}{(1+z)^8}+\frac{(1-z)^{16}}{(1+z)^{16}})$. Simplifying this, we get $W_{C^\perp} = \frac{1}{2^5}((1+z)^{16}+30(1-z^2)^8+(1-z)^{16}) = \frac{1}{32}(32+4480\,z^4+14336\,z^6+27840\,z^8+14336\,z^{10}+4480\,z^{12}+32\,z^{16}) = 1+140z^4+448z^6+870z^8+448z^{10}+140z^{12}+z^{16}$. This is the weight enumerator for the third order Reed Muller code of length 16. (NOTE: I used Mathematica, and in particular the command Expand, to help me with this answer.)

25 pts. **5** Use the MacWilliams identities to find the weight enumerator for the orthogonal code to the Nordstrom-Robinson code (which has 30 words of weight 8, 112 words of weight 6, 112 words of weight 10, 1 word of weight 16 and 1 word of weight 0).

$W_C(z) = 1+112z^6+30z^8+112z^{10}+z^{16}$: by the MacWilliams identities, $W_{C^\perp} = \frac{1}{2^8}(1+z)^{16}(1+112(\frac{1-z}{1+z})^6+30(\frac{1-z}{1+z})^8+112(\frac{1-z}{1+z})^{10}+(\frac{1-z}{1+z})^{16})$. Simplifying, we get $W_{C^\perp} = \frac{1}{256}(1+112(1-z)^6(1+z)^{10}+30(1-z)^8(1+z)^8+112(1-z)^{10}(1+z)^6+(1-z)^{16}) = 1+112z^6+30z^8+112z^{10}+z^{16}$. Note that $C^\perp$ has the same weight enumerator as C. Even though the code is not linear over Z_2, it is "formally self-dual". Jamie will explain to us in her project why this works!