Math 2^8: The Theory of Error-Correcting Codes
Problem Set #2

1. Let A be a finite field of q elements, and $n = (q^k - 1)/(q - 1)$ for some integer $k > 1$. Give a simple way to decode the perfect 1-error-correcting $[n, n-k, 3]$ Hamming code over A.

2. What is the dual of the classical Goppa $[q + 1, k + 1, q + 1 - k]$ MDS code?

3. i) Let Π be a combinatorial finite projective plane of *even* order q. Prove that any oval (set of $q + 1$ points with no three collinear) in Π extends to a hyperoval, i.e. that its $q+1$ tangents all meet at a point. [Hint: for each point P of Π off the oval let $\tau(P)$ be the number of tangents containing P. Prove that $\sum_P(\tau(P) - 1)(\tau(P) - q - 1) = 0$.]
   ii) In the case that q is a power of 2 and Π is the algebraic projective plane over the field of q elements, we proved (i) in class *for a conic* en route to Segre's theorem. Interpret this result (for arbitrary (hyper)ovals, conic or not) in terms of MDS codes.

4. Let F be a finite field of 2^n elements, and let d be an integer relatively prime to n. Prove that the subset of $\mathbf{P}^2(F)$ consisting of all points of the form $(x : y : z) = (a^{2^d} : a : 1)$ ($a \in F$) together with $(1 : 0 : 0)$ and $(0 : 1 : 0)$ is a hyperoval, and is an extended conic (a conic together with its center) if and only if $r \equiv \pm 1 \bmod d$. Conclude that if $n = 5$ or $n > 6$ then $\mathbf{P}^2(F)$ contains hyperovals which are not extended conics.

5. Let A be a finite field of odd order q. Prove that there exists a linear $[n, n - 4, 4]$ code over A for $n = q^2 + 1$ but not for $n > q^2 + 1$. NB: This is a more substantial exercise than the first three; to construct a $[q^2 + 1, q^2 - 3, 4]$ code you'll need to know about quadratic forms over finite fields.

   It is known that this $[q^2 + 1, q^2 - 3, 4]$ code is in fact unique up to the usual equivalence. For q even the maximum n is again $q^2 + 1$, but there may be more than one such code; this is related with Suzuki's family of simple groups ${}^2B_2(q)$!