1. Secret sharing schemes:

(a) Give a construction of a (4,2)-secret sharing scheme.

That is: assume that the secret is $s \in \{0,1\}$. Design a randomized scheme that assign shares to 4 players, such that any 2 of them can learn the secret, but any one individually cannot.

How large are your shares? How small can you get them to be?

(b) The construction of secret sharing schemes we saw in class all use randomness. Prove that this is indeed necessary; that is, there are no deterministic secret sharing schemes.

2. Vandermonde matrix:

Let $a_1, \ldots, a_n$ be elements in a field (for example, real numbers, or a finite field). The Vandermonde matrix is defined as

$$V = V(a_1, \ldots, a_n) = \begin{pmatrix} 1 & a_1 & (a_1)^{n-1} \\ 1 & a_2 & (a_2)^{n-1} \\ \vdots & \vdots & \vdots \\ 1 & a_n & (a_n)^{n-1} \end{pmatrix}$$

That is, $V_{i,j} = (a_i)^{j-1}$ for $1 \leq i, j \leq n$. We gave a proof sketch in class to the following theorem.

Theorem: $\det(V) = \prod_{i<j}(a_j - a_i)$.

In particular, if $a_1, \ldots, a_n$ are distinct then $V$ has full rank (and hence is invertible).

(a) Give a complete proof of the theorem.

(b) Prove that if $a_1, \ldots, a_n$ are distinct nonzero elements, then for any $k \geq 0$ the following matrix also has full rank: $M_{i,j} = (a_i)^{j+k}$.
Coding theory

3. Singleton bound for erasures

Let $C$ be any $(n,k,d)$ code. We saw in class the singleton bound for errors, which showed that any such code can correct up to $(d-1)/2$ errors. Prove that it can correct up to $d-1$ erasures (recall that erasures correspond to replacing a codeword symbol with a ?).

4. Asymptotically good linear codes

We recall some basic definitions: a linear binary code is a linear subspace $C \subseteq (\mathbb{Z}_2)^n$. It is an $(n,k,d)$ code if $|C| = 2^k$ and $\min(|x|: x \in C, x \neq 0) \geq d$, where $|x|$ denotes the hamming weight of $x \in \{0,1\}^n$ (that is, the number of 1’s in $x$).

The code $C$ is called a good code if $k \geq \alpha n, d \geq \beta n$ for some absolute constants $\alpha, \beta > 0$ (formally, we are talking about a family of codes, with fixed $\alpha, \beta > 0$ and $n \to \infty$).

We saw in class a proof that there exist non-linear good codes; specifically, that there exist $(n,k=n/10,d=n/10)$ codes for any large $n$.

Prove that there exist good linear codes.

Hint: show that a randomly chosen linear code is a good code, with high probability (for a suitable choice of $\alpha, \beta > 0$)

5. Reed-Solomon codes

Reed-Solomon codes are MDS codes. Here, we consider a specific example of $(17,14,3)$ code, which can be realized by a Reed-Muller code over the prime field $\mathbb{F}_{17}$. It can correct up to 1 error, or up to 2 erasures.

Write code (in your favorite programming language) that does the following:

(a) Encodes a message to a codeword

(b) Decodes a correct codeword to a message (assuming no errors or erasures)

(c) Decodes a codeword with up to 2 erasures

(d) Decodes a codeword with up to 1 errors (you don’t have to use the sophisticated algebraic algorithm we learned in class; any simpler, but less efficient algorithm, will do, if you can come up with one).