Problem 1. (Bivariate Interpolation) Let $F$ be a field and $F[x, y]_{m,n}$ denote the set of bivariate polynomials over $F$ whose degree in $x$ is at most $m$ and whose degree in $y$ is at most $n$.

1. What is the dimension of $F[x, y]_{m,n}$ as a vector space over $F$? Exhibit a basis for $F[x, y]_{m,n}$ over $F$.

2. Suppose $S \subseteq F^2$ is a set of fewer than $(m+1)(n+1)$ points in $F^2$. Show that there is a nonzero polynomial $p(x, y) \in F[x, y]_{m,n}$ such that $p(a, b) = 0$ for all $(a, b) \in S$. Explain how, given $S$, we could compute such a polynomial $p(x, y)$ using $\text{poly}(n + m)$ operations over $F$.

Problem 2. (Codes over Small Alphabets) The $q$-ary Hadamard code is the mapping $\text{Had} : F_k^q \to F_{kq}^q$ taking each $m \in F_k^q$ to the tuple $\langle (m, v_1), (m, v_2), \ldots, (m, v_{q^k}) \rangle$, where $v_1, \ldots, v_{q^k}$ are a list of all elements of $F_q^k$ and $\langle u, v \rangle = \sum_i u_i v_i$. That is, we view $m$ as describing a linear function from $F_q^k \to F_q$ and the codeword is the evaluation of this linear function at all points. This code has very poor relative rate $(k/q^k)$, but it has very good distance (as you will show) and can use very small alphabet sizes (even $q = 2$).

1. Show that the relative minimum distance of $\text{Had}$ is $1 - 1/q$. 
2. Combine a Reed-Solomon code over $\mathbb{F}_{2^\ell}$ for some $\ell$ and a Hadamard code to construct, for every $k = 2^\ell \geq 4$, an error-correcting code $\text{Enc} : \{0,1\}^k \to \{0,1\}^{k^2}$ with relative minimum distance at least $1/4$. (Hint: view elements of $\{0,1\}^k$ as elements of $(\mathbb{F}_{2^\ell})^{[k/\ell]}$, encode these in a Reed-Solomon code, and then encode each resulting symbol in a Hadamard code.)

The above code has much better rate $(1/k)$ than the Hadamard code, but still not constant. Nevertheless, this same approach of combining two codes ("code concatenation") is very widely used, and has been used to construct codes in which the rate, distance, and alphabet size are all constants independent of the message length $k$.

**Problem 3. (Improved Decoding of Reed–Solomon Codes)** Show that there is a polynomial-time algorithm for Noisy Polynomial Interpolation (see Lecture Notes 17) that works whenever the number $s$ of agreements is larger than $\sqrt{2dn}$, improving the $2d\sqrt{n}$ bound from lecture and the $2\sqrt{dn}$ bound from the lecture notes. You may ignore round-off issues in your solution, and treat quantities like $\sqrt{2n/d}$ as integers. (Hint: do not use fixed upper bounds on the individual degrees in $x$ and $y$ of the interpolating polynomial $Q(x,y)$, but rather allow as many monomials as possible for Step 2 to go through.)

**Problem 4. (Abstract Extension Fields [AM106])** Write out complete addition and multiplication tables for $\mathbb{Z}_2[x]/(x^3 + x + 1)$. (Due to commutativity, you only need to write the upper-triangular portion of these tables, including the main diagonal.)