Problem Set 1

- Due Date: **26 Sep, 2022**
- Turn in your problem sets electronically (LaTeX, pdf or text file) by email. If you submit handwritten solutions, start each problem on a fresh page.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Refering sources other than the text book and class notes is strongly discouraged. But if you do use an external source (eg., other text books, lecture notes, or any material available online), ACKNOWLEDGE all your sources (including collaborators) in your writeup. This will not affect your grades. However, not acknowledging will be treated as a serious case of academic dishonesty.
- The points for each problem are indicated on the side. The total for this set is 100.
- Be clear in your writing.

1. [**Guessing hats problem**] (2+4+2+7)

   There are n people in a room, each of whom is given a black/white hat chosen uniformly at random (and independent of the choices of all other people). Each person can see the hat colour of all other people, but not their own. Each person is asked if they wish to guess their own hat colour. They can either guess, or abstain. Each person makes their choice without knowledge of what the other people are doing (or, they can be thought of as submitting their guesses simultaneously). They either win collectively, or lose collectively. They win if all the people who don't abstain guess their hat colour correctly and at least one person does not abstain. They lose if all people abstain, or if some person guesses their colour incorrectly. Your goal below is to come up with a strategy that will allow the n people to win with pretty high probability. We begin with a simple warmup:

   (a) Argue that the n people can win with probability at least $\frac{1}{2}$.
   Next we will see how one can really bump up the probability of success with some careful modelling, and some knowledge of Hamming codes.

   (b) Let's say that a directed graph G is a subgraph of the n-dimensional hypercube if its vertex set is $\{0,1\}^n$ and if $u \to v$ is an edge in G ,then u and v differ in at most one coordinate. Let $K(G)$ be the number of vertices of G with in-degree at least one, and out-degree zero. Show that the probability of winning the hat problem equals the maximum, over directed subgraphs G of the n-dimensional hypercube, of $K(G)/2^n$.

   (c) Using the fact that the out-degree of any vertex is at most n, show that $K(G)/2^n$ is at most $\frac{n}{n+1}$ for any directed subgraph G of the n-dimensional hypercube.

   (d) Show that if $n = 2^r - 1$, then there exists a directed subgraph G of the n-dimensional hypercube with $K(G)/2^n = \frac{n}{n+1}$.
   Hint: This is where the Hamming code comes in.

2. [**New codes from existing codes**] (1+2+3+4+5)

   In this problem you will need to come up with some ways of constructing new codes from existing ones, and prove the following statements (recall that $[n, k, d]_q$ stands for an block-length n linear code over $\mathbb{F}_q$ of dimension k):

(a) If there exists an $[n,k,d]_q$ code ($d \geq 2$), then there also exists an $[n-1,k,d' \geq d-1]_q$ code.

(b) If there exists an $[n,k,d]_2$ code with d odd, then there also exists an $[n+1,k,d+1]_2$-code.

(c) If there exists an $[n,k,d]_q$ code, there there also exists an $[n-d,k-1,d' \geq \lceil d/q \rceil]_q$code. *Hint:* Drop the d positions corresponding to the support of a minimum weight codeword.)

(d) If there exists an $[n,k_1,d_1]_q$ code and an $[n,k_2,d_2]_q$ code, then there also exists a $[2n,k_1+k_2,\min(2d_1,d_2)]_q$ code.

(e) If there exists an $[n,k,d]_2$ code ($0 < d < n/2$), then for every $m \geq 1$, there also exists an $\left[n^m, k, \frac{n^m-(n-2d)^m}{2}\right]_2$ code.

Hint: Given an $n \times k$ generator matrix G for the code, consider the $n^m \times k$ generator matrix whose $(i_1, i_2, \ldots, i_m)$'th row is the sum of rows $i_1, i_2, \ldots, i_m$ of G . It is also more slick to use a ±1 notation for binary alphabet via the translation $b \to (-1)^b$ from $\{0,1\}$ to $\{1,-1\}$ and track the bias $\mathbb{E}_{i \in 1,\ldots,N}[x_i]$ of a string $x \in \{-1,1\}^N$ as a proxy for its relative Hamming weight.

3. **[Combinatorial proof of q-ary Plotkin bound]** (7+7+1)

In class, we gave a geometric proof of the Plotkin bound over the binary alphabet. The same proof can be extended to any q-ary alphabet. In this exercise we will prove the q-ary version of the Plotkin bound via a purely combinatorial proof.

If $\mathcal{C} \subseteq [q]^n$ is a code with distance d and if $d > \left(1 - \frac{1}{q}\right) n$, then $|\mathcal{C}| \leq \frac{qd}{qd-(q-1)n}$.

Given an $(n,k,d)_q$ code $\mathcal{C}$ with $d > \left(1 - \frac{1}{q}\right) n$, define

$$S = \sum_{c_1 \neq c_2 \in \mathcal{C}} \Delta(c_1, c_2).$$

For the rest of the problem, think of $\mathcal{C}$ as an $|\mathcal{C}| \times n$ matrix where each row corresponds to a codeword in $\mathcal{C}$. Now consider the following:

(a) Looking at the contribution of each column in the matrix above , argue that

$$S \leq \left(1 - \frac{1}{q}\right) n\mathcal{C}|^2.$$

(b) Looking at the contribution of the rows in the matrix above, argue that

$$S \geq |\mathcal{C}|(|\mathcal{C}|-1) \cdot d.$$

(c) Conclude the q-ary version of Plotkin's bound.

4. **[t-wise independent spaces]** (6+2+6+6)

For integers $1 \leq k \leq n$, call a (multi)set $S \subseteq \{0,1\}^n$ to be k-wise independent if for every $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ and $(a_1, a_2, \ldots, a_k) \in \{0,1\}^k$,

$$\Pr_{x \in S}[x_{i_1} = a_1 \wedge x_{i_2} = a_2 \wedge \cdots \wedge x_{i_k} = a_k] = \frac{1}{2^k}$$

where the probability is over an element x chosen uniformly at random from S . Small sample spaces of k-wise independent sets are of fundamental importance in derandomization. In this problem, you will see how codes can be used to construct k-wise independent sets of near-optimal size.

(a) Prove that any linear code $\mathcal{C}$ whose dual $\mathcal{C}^\perp$ has distance $d^\perp$ is $(d^\perp - 1)$-wise independent.

(b) Let H be the $(2^\ell - 1) \times \ell$ parity check matrix of a binary Hamming code. Show from the previous part that the collection of vectors $S = \{\mathbf{H}x \mid \mathbf{x} \in \{0,1\}^\ell\}$ forms a pairwise independent space.

(c) Using BCH codes, show how one can construct a $2t$ -wise independent subset of $\{0,1\}^n$ of size at most $(n+1)^t$ when n is of the form $2^m - 1$.

(d) Show that any pairwise independent space on n bits must contain at least $n+1$ points.

(e) [Extra credit] Prove an almost matching lower bound for the t-wise independence case. That is, any t-wise independent set $S \subseteq \{0,1\}^n$ satisfies

$$|S| \geq \sum_{i=0}^{\lfloor \frac{t}{2} \rfloor} \binom{n}{i}. \tag{1}$$

Hint: Find a set of linearly independent vectors in $\mathbb{R}^{|S|}$ of cardinality at least the R.H.S of (1). Specifically, for $T \subseteq \{1, 2, \ldots, n\}$ of size $\leq \lfloor t/2 \rfloor$, consider the $\langle \chi_T(x) \rangle_{x \in S}$ where $\chi_T(x) = (-1)^{\sum_{i \in T} x_i}$.

In class, we saw Gilbert's greedy construction of a general code, and Varshamov's probabilistic construction of a linear code demonstrating an achievable rate-distance tradeoff. In the following two exercises you will be analysing a greedy construction of a linear code, also due to Varshamov, and a probabilistic construction of a general code.

5. **[Greedy linear construction of Varshamov bound]** (4+8+8)

You can assume the following fact.

Fact: An $(n-k) \times n$ matrix H is the parity check matrix of an $[n,k,d]_q$ linear code iff every set of $d-1$ columns of H is linearly independent.

We will refer to the number of columns in H as $|H|$.

The construction is as follows:

Algorithm 1: Greedy construction of parity check matrix

Input: n, k, d such that

$$2^{n-k} > \mathrm{Vol}_2(n-1, d-2)$$

Output: An $(n-k) \times |H|$ matrix H

```
$H \leftarrow \emptyset$
while $|H| < n$ AND $\exists v \in \{0,1\}^{n-k}$ which cannot be expressed as the sum of $\ell$ columns for
  $\ell \leq d-2$ (that is, $v \neq h_1 + \cdots + h_\ell$ for all choices of columns $h_1, \ldots, h_\ell$ of $H$) do
    $H \leftarrow H \cup \{v\}$ (as a column)
return $H$
```

(a) Show that the code $\mathcal{C}$ with H as its parity check matrix (that is, $\mathcal{C} = \{y \in \{0,1\}^n \mid Hy = \mathbf{0}\}$) has $\Delta(\mathcal{C}) \geq d$.

(b) Observe that $\mathcal{C}$ has at least $2^{|H|-(n-k)}$ codewords. Show in fact that $|H| = n$ and hence that $\mathcal{C}$ has 2^k codewords. Hence, the code achieves the parameters given by the Gilbert-Varshamov bound.

(c) Compare the size of this code to Gilbert's greedy construction done in class. In particular, for $d = 3$, compare them against each other as well as Hamming's bound. Which is better?

6. **[Random codes and the Gilbert-Varshamov bound]** (7.5+7.5)

Here we will study the distance of a random code, and how to modify it so that meets the Gilbert-Varshamov bound.

(a) Let $R \in [0,1]$ and let $k = Rn$. Pick "codewords" $c_1, c_2, \ldots, c_{2^k}$ independently and uniformly at random from $\{0,1\}^n$, and set $\mathcal{C} = \{c_i : i \in [2^k]\}$. Show that for any δ satisfying $H(\delta) > 1 - 2R$, with probability $\to 1$ as $n \to \infty$, the distance of the code $\mathcal{C}$ at most δn. Thus for $R > 0$, such a randomly chosen code *does not* meet the Gilbert-Varshamov bound.

(b) Let R and $\mathcal{C}$ be as in the previous part and now let $\delta' \in [0,1]$ satisfy $H(\delta') > 1 - R$. Let $\mathcal{C}' = \{c_i \in \mathcal{C} \mid \forall j \in [i-1], d_H(c_i, c_j) \geq \delta' n\}$. Clearly the distance of $\mathcal{C}'$ is at least $\delta' n$. Show that for sufficiently large n, with probability $\geq 1/3$, $|\mathcal{C}'| \geq \frac{2^k}{3}$. Thus $\mathcal{C}'$ meets the Gilbert-Varshamov bound.