HW 1

Topics in Error-Correcting Codes (Fall 2022)
University of Toronto
Swastik Kopparty

Due: At the end of the semester.

Let $B(x, r)$ denote the ball of radius r around x. Let $|B_n(r)|$ denote the volume of the ball of radius r in $\{0, 1\}^n$.

1. We will see a very tiny improvement to the Gilbert-Varshamov bound. This predates BCH codes, and also works for codes over larger alphabets.

   Let $v_1, \ldots, v_r$ be a collection of vectors in $\mathbb{F}_2^t$ such that no $d-1$ of them are linearly dependent. Show that if $B_r(d-2) < 2^t$, then there exists a vector $w \in \mathbb{F}_2^t$ such that no $d-1$ vectors out of

   $$\{v_1, \ldots, v_r, w\}$$

   are linearly dependent.

   Use this to show that for all d, for infinitely many n, there exists a linear code $C \subseteq \mathbb{F}_2^n$ with minimum distance $\geq d$ such that $|C| \geq \frac{2^n}{|B_n(d-2)|}$.

2. Let $q > 2$ be a prime power (you can restrict to q being a prime if you are not yet comfortable with general finite fields). Generalize the Hamming code over $\mathbb{F}_2$ that we saw in class to construct (for suitable n) a distance ≥ 3 error-correcting code $C \subseteq \mathbb{F}_q^n$ with $|C| \geq \frac{q^n}{(q-1)n+1}$.

   This shows that the volume packing bound is tight even over prime power sized alphabets and $d = 3$.

3. **(Not to be turned in)** Review all your linear algebra, but this time pay attention to which facts hold over finite fields, and which facts don't.

4. **(Not to be turned in)** Let $x \in \{0, 1\}^n$. For $r = 100, \sqrt{n}, 0.1n, n/2, 0.9n$, solve the following problem. Let z be a point picked uniformly at random from $B(x, r)$. Estimate the probability that $\Delta(z, x) = r$.

   The answers are: $1 - O(1/n), 1 - O(1/\sqrt{n})$, constant $p \in (0, 1)$, $O(1/\sqrt{n})$, $2^{-\Theta(n)}$.

5. **(Not to be turned in)** Below is a collection of facts/problems related to finite fields. Try to verify them yourself or look them up.

   (a) Let p be prime. Let $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ along with operations addition and multiplication mod p. Every integer can be treated as an element of $\mathbb{F}_p$ (by taking the remainder after dividing by p).

   All of $\mathbb{F}_p$ forms a group under addition. The nonzero elements of $\mathbb{F}_p$, denoted $\mathbb{F}_p^*$ form a group under multiplication. Both groups are commutative.

   (b) For each $a \in \mathbb{F}_p$, we have $a^p = a$. If $a \neq 0$, then $a^{p-1} = 1$.

(c) Let $\mathbb{F}_p[X]$ be the set of polynomials with $\mathbb{F}_p$ coefficients. Then the division theorem holds in $\mathbb{F}_p[X]$, and thus every element of $\mathbb{F}_p[X]$ can be uniquely factorized into irreducible polynomials.

(d) The remainder theorem holds in $\mathbb{F}_p[X]$. Thus $X^p - X = \prod_{\alpha \in \mathbb{F}_p}(X - \alpha)$.

(e) For each integer d, the number of $a \in \mathbb{F}_p^*$ satisfying $a^d = 1$ is at most d. Combining this with the fact that $\mathbb{F}_p^*$ is commutative, this implies that $\mathbb{F}_p^*$ is cyclic (i.e., there is an element $g \in \mathbb{F}_p^*$ such that $\mathbb{F}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$.

Not every element of $\mathbb{F}_p^*$ generates $\mathbb{F}_p^*$. Look at the cases $p = 7, 13$ and find a generator for $\mathbb{F}_p^*$ in each case.

(f) Suppose p is an odd prime. Then exactly $1/2$ the elements of $\mathbb{F}_p^*$ are perfect squares. If $a \in \mathbb{F}_p^*$, then $a^{(p-1)/2}$ equals either 1 or -1, depending on whether a is a perfect square or not.

(g) Generalize the above to perfect dth powers. Note that if d is relatively prime to $p-1$ then every element of $\mathbb{F}_p^*$ is a perfect dth power.

(h) Let $f(X)$ be an irreducible polynomial of degree d in $\mathbb{F}_p[X]$. We can consider the set $\mathbb{F}_p[X]/f(X)$ of polynomials modulo $f(X)$. Every polynomial is equivalent modulo $f(X)$ to a unique polynomial of degree $< d$. Thus there are p^d residue classes. Addition and multiplication of polynomials is compatible with reducing mod $f(X)$. Every nonzero element of $\mathbb{F}_p[X]/f(X)$ has a multiplicative inverse (this is where irreducibility of $f(X)$ is used). Thus $\mathbb{F}_p[X]/f(X)$ is a field of cardinality p^d.

The relationship between $\mathbb{Z}$, the prime p and the field $\mathbb{Z}/p$ is entirely analogous to the relationship between $\mathbb{F}_p[X]$, the irreducible $f(X)$ and the field $\mathbb{F}_p[X]/f(X)$.

(i) The field $\mathbb{F}_p[X]/f(X)$ is a d-dimensional vector space over the field $\mathbb{F}_p$. We denote this field $\mathbb{F}_{p^d}$. It is tricky to prove but true that any two fields of cardinality p^d are isomorphic fields. Thus there is a unique such field. If n is an integer not of the form p^d for p prime, then there does not exist a finite field of cardinality n. Thus whenever we talk of the finite field $\mathbb{F}_q$, we will insist that q be a prime power.

(j) Note that the above construction of $\mathbb{F}_{p^d}$ required the existence of an irreducible polynomial of degree d over $\mathbb{F}_p$. Such polynomials exist for every d! Try to show this.

(k) Construct the fields $\mathbb{F}_8$ and $\mathbb{F}_9$.

(l) Note that the field $\mathbb{F}_{p^d}$ is not isomorphic to the ring $\mathbb{Z}/p^d$.

(m) Many of the facts you proved about the field $\mathbb{F}_p$ also hold for $\mathbb{F}_{p^d}$. Polynomials over $\mathbb{F}_{p^d}$ can be defined, and they have nice properties. The multiplicative group $\mathbb{F}_{p^d} \setminus \{0\}$ is cyclic. Etc. To prove all these properties, you need not use the explicit construction of $\mathbb{F}_{p^d}$ described above. It suffices to just use the fact that $\mathbb{F}_{p^d}$ is a field of cardinality p^d.

(n) $X^{p^d} - X = \prod_{\alpha \in \mathbb{F}_{p^d}}(X - \alpha)$.

6. Let C be a Reed-Solomon code over $\mathbb{F}_q$ with length N and distance D.

(a) Let $c \in C$. Suppose x is a received word obtained from c after r errors and s erasures occur.

Give a polynomial time algorithm, which on input x can recover c, provided:

$$r + \frac{s}{2} < \frac{D}{2}.$$

(b) Let $c \in C$. Let $x \in \mathbb{F}_q^N$ and $u \in [0,1]^N$: we will view u_i as the amount of "uncertainty" in the symbol x_i ($u_i = 1$ is like an erasure). For each $i \in [N]$, define err_i by:

$$err_i = \begin{cases} 1 - u_i/2 & x_i \neq c_i \\ u_i/2 & x_i = c_i \end{cases}$$

Give a polynomial time algorithm, which on input x and u can recover c, provided:

$$\sum_{i \in [N]} err_i < \frac{D}{2}.$$

A hint for this available at the end of the problem set.

(c) Let $C_{in} \subseteq \{0,1\}^n$ be a binary code with q codewords. Let d be the minimum distance of C_{in}. Let V be the concatenated code obtained by concatenating C with C_{in}. Recall that V has minimum distance $\geq D \cdot d$.

Here is an algorithm for decoding V from $\frac{D \cdot d}{2}$ errors.

i. Let $y_1, y_2, \ldots, y_N \in \{0,1\}^n$ be the blocks of the received vector y.

ii. Decode each y_i from up to $d/2$ errors to obtain a codeword $c_i \in C_{in}$. Let $a_i = \Delta(y_i, c_i)$.

iii. Let $x_i \in \mathbb{F}_q$ be the $\mathbb{F}_q$-symbol corresponding to c_i. Let $u_i = \frac{a_i}{d/2}$.

iv. Then (x, u) satisfy the hypothesis for the previous part of this problem. Decode this to obtain the codeword c.

Show that this algorithm works.

7. For each $R \in (0,1)$, show that there exist linear codes $C \subseteq \mathbb{F}_2^n$ such that both C and $C^\perp$ meet the Gilbert-Varshamov bound.

8. Covering codes.

(a) A code $C \subseteq \{0,1\}^n$ is called a covering code with covering radius r if for every $x \in \{0,1\}^n$, there exists some $c \in C$ with $\Delta(x, c) \leq r$.

Let $\rho \in (0, 1/2)$ be a constant. Show that every covering code $C \subseteq \{0,1\}^n$ with covering radius ρn has rate $R \geq 1 - H(\rho) - o(1)$.

(b) Show that choosing 2^{Rn} independent uniform elements of $\{0,1\}^n$, if $R \leq 1 - H(\rho) + o(1)$, is a covering code with covering radious ρn with high probability.

Thus the the main combinatorial questions for covering codes are much easier than for error-correcting codes.

(c) In fact, one can even construct such covering codes efficiently! Here is the construction.

Let n' be an integer. Let R, ρ, ϵ be such that $R = 1 - H(\rho) + \epsilon$. Let $M = (2^{n'})^{2^{Rn'}}$. Let $C_1, C_2, \ldots, C_M$ be an enumeration of ALL 2^{Rn}-tuples of elements of $\{0,1\}^n$.

Let $n = M \cdot n'$. Define

$$C = \{(x_1, \ldots, x_M) \in \{0,1\}^n \mid x_i \in C_i\},$$

where we identify elements of $\left(\{0,1\}^M\right)^{n'}$ with $\{0,1\}^n$.
Show that C is a covering code with rate R and covering radius $\rho + o(1)$.

Hint for weighted Reed-Solomon decoding: reduce to errors-and-erasures decoding.