HW 1

Error-Correcting Codes (Spring 2016)
Rutgers University
Swastik Kopparty

Due: Feb 4, 2016

If you need permission to register for the course, submit problems 1 and 2 to me by email by Tuesday, Jan 26.

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. This problem will give another proof that there exist codes of size $\Omega(\frac{2^n}{|B_n(d-1)|})$ with minimum distance $\geq d$.

   Let $x_1, x_2, \ldots, x_K$ be picked independently and uniformly at random from $\{0,1\}^n$.

   (a) Let A be the expected number of pairs $\{i,j\} \subseteq \{1,\ldots,K\}$ such that $\Delta(x_i, x_j) < d$. Compute A.

   (b) Show that if $K = \frac{2^n}{10|B_n(d-1)|}$ then $A < K/2$.

   (c) Use this to show that there exists a code C with minimum distance d with $|C| \geq \frac{1}{20} \cdot \frac{2^n}{|B_n(d-1)|}$.

2. The goal of this problem is to construct (inefficiently) a large *linear* code with minimum distance $\geq d$. In class we saw a greedy procedure to do this without the linearity constraint.

   Let $C \subseteq \mathbb{F}_2^n$ be a linear code with minimum distance $\geq d$. Show that if $|C| < \frac{2^n}{|B_n(d-1)|}$, then there exists an $x \in \mathbb{F}_2^n$ such that the linear space generated by C and x has minimum distance $\geq d$.

   Use this to prove that there exist linear codes C with $|C| \geq \frac{2^n}{|B_n(d-1)|}$.

3. We will see an improvement to the previous argument, to get a slightly larger linear code.

   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 $|C| \geq \frac{2^n}{|B_n(d-2)|}$.

4. Let d be an odd integer.

   Suppose $C \subseteq \mathbb{F}_2^n$ is a linear code with minimum distance $\geq d$.

   Show that there exists a linear code $C' \subseteq \mathbb{F}_2^n$ with minimum distance $\geq d+1$ such that $|C'| \geq |C|/2$.

   Apply the above transformation to the Hamming code. This is called the extended Hamming code.

5. 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 $d = 3$.

6. **(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.

7. **(Not to be turned in)** Show that there do not exist 4 vectors in $\{0,1\}^n$ with pairwise distance $\geq 2/3n$.

8. **(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 $p \in (0,1)$, $O(1/\sqrt{n})$, $2^{-\Theta(n)}$.

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