Summary on Lecture 17, May 6th, 2016

Introduction to coding theory.

Here we describe basics of coding theory. Assume we have to transmit a binary signal, i.e. a string $\mathbf{w}$ of 0's and 1's, say $\mathbf{w} = 011010110$. We have to expect that there is a "noise" during this submition, and we have to use some techniques to correct an error.

Example. Assume we send a string $\mathbf{w} = 011010110$. We can identify $\mathbf{w}$ with the element $(0,1,1,0,1,0,1,1,0)$ of the cartisian product

$$\mathbf{Z}_2^9 = \underbrace{\mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2}_{9}.$$

Suppose the message we received is $\mathbf{v} = (0,1,1,0,1,1,1,0,0) \in \mathbf{Z}_2^9$ which is not the message we sent. This give us the error $\mathbf{e} = (0,0,0,0,0,1,0,1,0)$, where the entry 1 indicates the error during the transmission. Now we can write the identity in $\mathbf{Z}_2^9$:

$$\mathbf{w} - \mathbf{v} = \mathbf{e} \quad \text{or} \quad \mathbf{v} + \mathbf{w} = \mathbf{e}.$$

Now we assume that for each digit of $\mathbf{w}$ there is probability p of incorrect transmission. We also assume that the transmission of any signal does not in any way depend on the transmission of prior signals. Then there is a probability

$$(1-p)^5 p(1-p)p(1-p) = (1-p)^7 p^2$$

of having the error $e = (0,0,0,0,0,1,0,1,0)$.

Now we describe a general construction. Let $\mathbf{w} = w_1 \dots w_n \in \{0,1\}^n$ be a message to be transmitted. We identify $\mathbf{w}$ with an element in $\mathbf{Z}_2^n$, i.e., we write

$$\mathbf{w} = (w_1, \dots, w_n) \in \mathbf{Z}_2^n.$$

Then we denote by $\mathbf{v} = (v_1, \dots, v_n)$ the received message, and by $\mathbf{e} = (e_1, \dots, e_n)$ the error, i.e., $\mathbf{e} = \mathbf{w} + \mathbf{v}$. Here is our general observation:

Lemma 1. *Assume that for each digit of $\mathbf{w}$ there is probability p of incorrect transmission, and that the transmission of any signal does not in any way depend on the transmission of prior signals.*

(1) *The probability that the error $\mathbf{e} \in \mathbf{Z}_2^n$ has a particular pattern with k 1's and $(n-k)$ 0', is $p^k(1-p)^{n-k}$.*

(2) *The probability that the error $\mathbf{e} \in \mathbf{Z}_2^n$ has exactly k 1's and $(n-k)$ 0', is $\binom{n}{k} p^k(1-p)^{n-k}$.*

We notice that the probability to have an error in two entries is much smaller than to have an error in one entry. Say, if $p = 0.01 = 10^{-2}$, the probability to have two errors is

$$\binom{n}{2} 10^{-4}(1-10^{-2})^{n-2} \cong \binom{n}{2} 10^{-4}\left(1-(n-2)10^{-2(n-2)}\right) \cong \binom{n}{2} 10^{-4} = \frac{n(n-1)}{2} 10^{-4},$$

which much smaller comparing with the probability to have just one error $n \cdot 10^{-2}$.

Improvement to Accuracy. Let m be the length of the signals to be transmitted. The idea is to increase the length from m to $n >> m$ as follows. First, we choose an *encoding function* $\alpha : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$. The set $C = \alpha(\mathbf{Z}_2^m) \subset \mathbf{Z}_2^n$ is called the *code*, and its elements are called the *code words*.

Example 1. Let $\alpha : \mathbf{Z}_2^n \to \mathbf{Z}_2^{n+1}$ is given as

$$\alpha : (w_1, \dots, w_n) \mapsto (w_1, \dots, w_n, w_1 + \cdots + w_n)$$

Let q be a number of 1's in $\mathbf{w} = (w_1, \dots, w_n)$. Then last digit of $\alpha(\mathbf{w})$ is q mod 2. It means that $\alpha(\mathbf{w}) \in \mathbf{Z}_2^{n+1}$ has always even number of 1's.

Now we make a transmission $\tau : \mathbf{Z}_2^{n+1} \to \mathbf{Z}_2^{n+1}$, and let $\mathbf{v} = \tau(\mathbf{w})$. Assume that the transmission τ went with an error in one entry. Then the message $\mathbf{v} = \tau(\mathbf{w})$ has odd number of 1's; thus we know for sure that there is an error in the transmission. Here we can detect the error, but we have no means to correct it.

Example 2. Let $\alpha : \mathbf{Z}_2^n \to \mathbf{Z}_2^{3n}$ is given as

$$\alpha : (w_1, \dots, w_n) \mapsto (w_1, \dots, w_n, w_1, \dots, w_n, w_1, \dots, w_n),$$

i.e. we just repeat $\mathbf{w}$ two more times. Now we make a transmission $\tau : \mathbf{Z}_2^{3n} \to \mathbf{Z}_2^{3n}$, and let

$$\mathbf{v} = \tau(\mathbf{w}) = (v_1, \dots, v_n, v_1', \dots, v_n', v_1'', \dots, v_n'').$$

Then we use the following decoding function $\sigma : \mathbf{Z}_2^{3n} \to \mathbf{Z}_2^n$:

$$(v_1, \dots, v_n, v_1', \dots, v_n', v_1'', \dots, v_n'') \mapsto (u_1, \dots, u_n),$$

where u_j is equal to the majority of the elements v_j, v_j', v_j''. Clearly if at most one entry among v_j, v_j', v_j'' is different from w_j, then we still have $u_j = w_j$. Thus we correct the message if there is an error in just one entry.

The Hamming metric. Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{Z}_2^n$. Then we define a weight $\omega(\mathbf{x})$ as a number of non-zero entries x_i.

Definition 1. Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{Z}_2^n$ and $\mathbf{y} = (y_1, \dots, y_n) \in \mathbf{Z}_2^n$. Then the distance between $\mathbf{x}$ and $\mathbf{y}$ is given as

$$\delta(\mathbf{x}, \mathbf{y}) = |\{ \ j \mid x_j \neq y_j \ \}|,$$

i.e., $\delta(\mathbf{x}, \mathbf{y})$ is the number of corresponding entries of $\mathbf{x}$ and $\mathbf{y}$ which are different.

Lemma 1. *Let $\mathbf{x}, \mathbf{y} \in \mathbf{Z}_2^n$. Then $\delta(\mathbf{x}, \mathbf{y}) = \omega(\mathbf{x} + \mathbf{y})$.*

Proof. We note that $x_j \neq y_j$ if and only if $x_j + y_j = 1 \mod 2$. □

Lemma 2. *Let $\mathbf{x}, \mathbf{y} \in \mathbf{Z}_2^n$. Then $\omega(\mathbf{x} + \mathbf{y}) \leq \omega(\mathbf{x}) + \omega(\mathbf{y})$.*

Proof. Let $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$, and $\mathbf{z} = \mathbf{x} + \mathbf{y} = (z_1, \dots, z_n)$. Then it is easy to check that $z_j \leq x_j + y_j \mod 2$. Indeed, if at least one of x_j, y_j is not equal to one, then $z_j = x_j + y_j$. If $x_j = 1$ and $y_j = 1$, then $z_j = 0 \mod 2$. It means that the number of 1's in $\mathbf{z}$ is less or equal to the sum of number of 1's of $\mathbf{x}$ and $\mathbf{y}$. □

Theorem 1. *The distance function $\delta : \mathbf{Z}_2^n \times \mathbf{Z}_2^n \to \mathbf{Z}_{\geq 0}$ satisfies the following properties:*

(1) $\delta(\mathbf{x}, \mathbf{y}) \geq 0$;
(2) $\delta(\mathbf{x}, \mathbf{y}) = 0$ *if and only if* $\mathbf{x} = \mathbf{y}$;
(3) $\delta(\mathbf{x}, \mathbf{y}) = \delta(\mathbf{y}, \mathbf{x})$;
(4) $\delta(\mathbf{x}, \mathbf{z}) \leq \delta(\mathbf{x}, \mathbf{y}) + \delta(\mathbf{y}, \mathbf{z})$.

Exercises. Prove Theorem 1.

The pair $(\mathbf{Z}_2^n, \delta)$ is an example of a *metric space*.

Definition. Let $r \geq 1$ be a positive integer, and $\mathbf{x} \in \mathbf{Z}_2^n$. Then the set $B_r(\mathbf{x}) = \{ \ \mathbf{y} \mid \delta(\mathbf{x}, \mathbf{y}) \leq r \ \}$ is called a *closed ball of radius* r.

Theorem 2. *Let $m, n \in \mathbf{Z}_+$, and $m < n$. Assume $\alpha : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ be an encoding function, such that $C = \alpha(\mathbf{Z}_2^m) \subset \mathbf{Z}_2^n$.*

(a) *If $\delta(\mathbf{x}, \mathbf{y}) > r$ for all strings in C with $\mathbf{x} \neq \mathbf{y}$, then a transmission τ with $\delta(\mathbf{c}, \tau(\mathbf{c})) \leq r$ can always be detected, i.e., a transmission with at most r errors can always be detected.*
(b) *If $\delta(\mathbf{x}, \mathbf{y}) > 2r$ for all strings in C with $\mathbf{x} \neq \mathbf{y}$, then a transmission τ with $\delta(\mathbf{c}, \tau(\mathbf{c})) \leq r$ can always be detected and corrected.*

Proof. (a) Let $\mathbf{c} \in C$ and we consider the ball $B_r(\mathbf{c})$. Then, since $\delta(\mathbf{x}, \mathbf{y}) > r$ for all strings in C with $\mathbf{x} \neq \mathbf{y}$, we have that $B_r(\mathbf{c}) \cap C = \{\mathbf{c}\}$: indeed, all other elements of C are further away from the center $\mathbf{c}$ of the ball. It means that for any transmission with number of errors between 1 and r we should have that $\tau(\mathbf{c}) \neq \mathbf{c}$, and $\tau(\mathbf{c}) \in B_r(\mathbf{c})$. We obtain that $\tau(\mathbf{c}) \notin C$. This means that such an error could be detected.

(b) As we have seen, the condition $\delta(\mathbf{x}, \mathbf{y}) > 2r$ for all strings in C with $\mathbf{x} \neq \mathbf{y}$ implies that for any transmission with number of errors between 1 and r we should have that $\tau(\mathbf{c}) \neq \mathbf{c}$, and $\tau(\mathbf{c}) \in B_r(\mathbf{c})$. On the other hand, for every $\mathbf{x} \in C$ such that $\mathbf{x} \neq \mathbf{c}$, $2r < \delta(\mathbf{c}, \mathbf{x}) \leq \delta(\mathbf{c}, \tau(\mathbf{c})) + \delta(\tau(\mathbf{c}), \mathbf{x})$. By assumption, $\delta(\mathbf{c}, \tau(\mathbf{c})) < r$. Then it means that $\delta(\tau(\mathbf{c}), \mathbf{x}) > r$, or that $\tau(\mathbf{c}) \notin B_r(\mathbf{x})$. Since $\tau(\mathbf{c}) \in B_r(\mathbf{c})$, it means that $\mathbf{c}$ is the only element of C which could be transmitted to $\tau(\mathbf{c})$. □