Chapter 29

Shannon’s theorem

By Sariel Har-Peled, September 14, 2018

“...This has been a novel about some people who were punished entirely too much for what they did. They
wanted to have a good time, but they were like children playing in the street: they could see one after
another of them being killed - run over, maimed, destroyed - but they continued to play anyhow. We really
all were very happy for a while, sitting around not toiling but just bullshitting and playing, but it was for
such a terrible brief time, and then the punishment was beyond belief; even when we could see it, we could
not believe it.”

– – A Scanner Darkly, Philip K. Dick.

29.1. Coding: Shannon’s Theorem

We are interested in the problem sending messages over a noisy channel. We will assume that the
channel noise is behave “nicely”.

Definition 29.1.1. The input to a binary symmetric channel with parameter $p$ is a sequence of bits
$x_1, x_2, \ldots$, and the output is a sequence of bits $y_1, y_2, \ldots$, such that $P[x_i = y_i] = 1 - p$ independently for
each $i$.

Translation: Every bit transmitted have the same probability to be flipped by the channel. The
question is how much information can we send on the channel with this level of noise. Naturally, a
channel would have some capacity constraints (say, at most 4,000 bits per second can be sent on the
channel), and the question is how to send the largest amount of information, so that the receiver can
recover the original information sent.

Now, its important to realize that handling noise is unavoidable in the real world. Furthermore,
there are tradeoffs between channel capacity and noise levels (i.e., we might be able to send considerably
more bits on the channel but the probability of flipping [i.e., $p$] might be much larger). In designing a
communication protocol over this channel, we need to figure out where is the optimal choice as far as
the amount of information sent.

Definition 29.1.2. A $(k,n)$ encoding function $Enc : \{0,1\}^k \to \{0,1\}^n$ takes as input a sequence of $k$
bits and outputs a sequence of $n$ bits. A $(k,n)$ decoding function $Dec : \{0,1\}^n \to \{0,1\}^k$ takes as input a sequence of $n$ bits and outputs a sequence of $k$ bits.

Thus, the sender would use the encoding function to send its message, and the receiver would use
the transmitted string (with the noise in it), to recover the original message. Thus, the sender starts
with a message with $k$ bits, it blow it up to $n$ bits, using the encoding function (to get some robustness

\footnote{This work is licensed under the Creative Commons Attribution-Noncommercial 3.0 License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.}
to noise), it send it over the (noisy) channel to the receiver. The receiver takes the given (noisy) message with \( n \) bits, and use the decoding function to recover the original \( k \) bits of the message.

Naturally, we would like \( k \) to be as large as possible (for a fixed \( n \)), so that we can send as much information as possible on the channel.

The following celebrated result of Shannon\(^2\) in 1948 states exactly how much information can be sent on such a channel.

**Theorem 29.1.3 (Shannon’s theorem).** For a binary symmetric channel with parameter \( p < 1/2 \) and for any constants \( \delta, \gamma > 0 \), where \( n \) is sufficiently large, the following holds:

(i) For an \( k \leq n(1-H(p)-\delta) \) there exists \((k,n)\) encoding and decoding functions such that the probability the receiver fails to obtain the correct message is at most \( \gamma \) for every possible \( k \)-bit input messages.

(ii) There are no \((k,n)\) encoding and decoding functions with \( k \geq n(1-H(p)+\delta) \) such that the probability of decoding correctly is at least \( \gamma \) for a \( k \)-bit input message chosen uniformly at random.

### 29.1.0.1. Intuition behind Shanon’s theorem

Let assume the senders has sent a string \( S = s_1s_2\ldots s_n \). The receiver got a string \( T = t_1t_2\ldots t_n \), where \( p = \mathbb{P}[t_i \neq s_i] \), for all \( i \). In particular, let \( U \) be the Hamming distance between \( S \) and \( T \); that is, \( U = \sum |s_i \neq t_i| \). Under our assumptions \( \mathbb{E}[U] = np \), and \( U \) is a binomial variable. By Chernoff inequality, we know that \( U \in [(1-\delta)np,(1+\delta)np] \) with high probability, where \( \delta \) is some tiny constant. So lets assume this indeed happens. This means that \( T \) is in a ring \( R \) centered at \( S \), with inner radius \((1-\delta)np\) and outer radius \((1+\delta)np\). This ring has

\[
\sum_{i=(1-\delta)np}^{(1+\delta)np} \binom{n}{i} \leq 2 \binom{n}{(1+\delta)np} \leq 2^{nH((1+\delta)p)}.
\]

Let us pick as many rings as possible in the hypercube so that they are disjoint: \( R_1,\ldots, R_\kappa \). If somehow magically, every word in the hypercube would be covered, then we could use all the possible \( 2^n \) codewords, then the number of rings \( \kappa \) we would pick would be at least

\[
k \geq \frac{2^n}{|R|} \geq \frac{2^n}{2^{nH((1+\delta)p)}} \approx 2^{n(1-H((1+\delta)p))}.
\]

In particular, consider all possible strings of length \( k \) such that \( 2^k \leq \kappa \). We map the \( i \)th string in \( \{0,1\}^k \) to the center \( C_i \) of the \( i \)th ring \( R_i \). Assuming that when we send \( C_i \), the receiver gets a string in \( R_i \), then the decoding is easy - find the ring \( R_i \) containing the received string, take its center string \( C_i \), and output the original string it was mapped to. Now, observe that

\[
k = \lfloor \log \kappa \rfloor = n(1-H((1+\delta)p)) \approx n(1-H(p)),
\]

as desired.

### 29.1.0.2. What is wrong with the above?

The problem is that we can not find such a large set of disjoint rings. The reason is that when you pack rings (or balls) you are going to have wasted spaces around. To overcome this, we would allow rings to overlap somewhat. That makes things considerably more involved. The details follow.

---

\(^2\)Claude Elwood Shannon (April 30, 1916 - February 24, 2001), an American electrical engineer and mathematician, has been called “the father of information theory”.
29.2. Proof of Shannon’s theorem

The proof is not hard, but requires some care, and we will break it into parts.

29.2.1. How to encode and decode efficiently

29.2.1.1. The scheme

Our scheme would be simple. Pick \( k \leq n(1 - \overline{H}(p) - \delta) \). For any number \( i = 0, \ldots, \hat{K} = 2^{k+1} - 1 \), randomly generate a binary string \( Y_i \) made out of \( n \) bits, each one chosen independently and uniformly. Let \( Y_0, \ldots, Y_{\hat{K}} \) denote these code words. Here, we have

\[
\hat{K} = 2^{n(1-\overline{H}(p)-\delta)}.
\]

For each of these codewords we will compute the probability that if we send this codeword, the receiver would fail. Let \( X_0, \ldots, X_K \), where \( K = 2^k - 1 \), be the \( K \) codewords with the lowest probability to fail. We assign these words to the \( 2^k \) messages we need to encode in an arbitrary fashion.

The decoding of a message \( w \) is done by going over all the codewords, and finding all the codewords that are in (Hamming) distance in the range \([p(1-\varepsilon)n, p(1+\varepsilon)n]\) from \( w \). If there is only a single word \( X_i \) with this property, we return \( i \) as the decoded word. Otherwise, if there are no such words or there is more than one word, the decoder stops and report an error.

29.2.1.2. The proof

Intuition. Let \( S_i \) be all the binary strings (of length \( n \)) such that if the receiver gets this word, it would decipher it to be \( i \) (here are still using the extended codeword \( Y_0, \ldots, Y_{\hat{K}} \)). Note, that if we remove some codewords from consideration, the set \( S_i \) just increases in size. Let \( W_i \) be the probability that \( X_i \) was sent, but it was not deciphered correctly. Formally, let \( r \) denote the received word. We have that

\[
W_i = \sum_{r \in S_i} P[r \text{ received when } X_i \text{ was sent}].
\]

To bound this quantity, let \( \Delta(x, y) \) denote the Hamming distance between the binary strings \( x \) and \( y \). Clearly, if \( x \) was sent the probability that \( y \) was received is

\[
w(x, y) = p^{\Delta(x, y)}(1 - p)^{n - \Delta(x, y)}.
\]

As such, we have

\[
P[r \text{ received when } X_i \text{ was sent}] = w(X_i, r).
\]

Let \( S_{i,r} \) be an indicator variable which is 1 if \( r \not\in S_i \). We have that

\[
W_i = \sum_{r \not\in S_i} P[r \text{ received when } X_i \text{ was sent}] = \sum_{r \not\in S_i} w(X_i, r) = \sum_r S_{i,r} w(X_i, r).
\]

The value of \( W_i \) is a random variable of our choice of \( Y_0, \ldots, Y_{\hat{K}} \). As such, its natural to ask what is the expected value of \( W_i \).

Consider the ring

\[
R(r) = \left\{ x \left| (1 - \varepsilon)np \leq \Delta(x, r) \leq (1 + \varepsilon)np \right\} ,
\]

where \( \varepsilon > 0 \) is a small enough constant. Suppose, that the code word \( Y_i \) was sent, and \( r \) was received. The decoder return \( i \) if \( Y_i \) is the only codeword that falls inside \( R(r) \).
Lemma 29.2.1. Given that $Y_i$ was sent, and $r$ was received and furthermore $r \in R(Y_i)$, then the probability of the decoder failing, is
\[
\tau = \mathbb{P}\left[ r \notin S_i \mid r \in R(Y_i) \right] \leq \frac{\gamma}{8},
\]
where $\gamma$ is the parameter of Theorem 29.1.3.

Proof: The decoder fails here, only if $R(r)$ contains some other codeword $Y_j$ ($j \neq i$) in it. As such,
\[
\tau = \mathbb{P}\left[ r \notin S_i \mid r \in R(Y_i) \right] \leq \mathbb{P}\left[ Y_j \in R(r), \text{ for any } j \neq i \right] \leq \sum_{j \neq i} \mathbb{P}\left[ Y_j \in R(r) \right].
\]
Now, we remind the reader that the $Y_j$s are generated by picking each bit randomly and independently, with probability $1/2$. As such, we have
\[
\mathbb{P}\left[ Y_j \in R(r) \right] = \sum_{m=(1-\varepsilon)n p}^{(1+\varepsilon)n p} \frac{n}{2^n} \leq \frac{n}{2^n} \left( 1 + \varepsilon np \right),
\]
since $(1 + \varepsilon)p < 1/2$ (for $\varepsilon$ sufficiently small), and as such the last binomial coefficient in this summation is the largest. By Corollary 29.3.2 (i), we have
\[
\mathbb{P}\left[ Y_j \in R(r) \right] \leq \frac{n}{2^n} \left( 1 + \varepsilon np \right) \leq \frac{n}{2^n} 2^n \left( 1 + \varepsilon (1+\varepsilon)p \right) = n 2^{n \left( \mathbb{H}(1+\varepsilon)p \right) - 1}.
\]
As such, we have
\[
\tau = \mathbb{P}\left[ r \notin S_i \mid r \in R(Y_i) \right] \leq \sum_{j \neq i} \mathbb{P}\left[ Y_j \in R(r) \right]
\leq \hat{K} \mathbb{P}[Y_1 \in R(r)] \leq 2^{k+1} n 2^{n \left( \mathbb{H}(1+\varepsilon)p \right) - 1}
\leq n 2^{n \left( 1 - \mathbb{H}(p) - \delta \right) + 1} n 2^{n \left( \mathbb{H}(1+\varepsilon)p \right) - 1} \leq n 2^{n \left( \mathbb{H}(1+\varepsilon)p - \mathbb{H}(p) - \delta \right) + 1}
\]
since $k \leq n(1 - \mathbb{H}(p) - \delta)$. Now, we choose $\varepsilon$ to be a small enough constant, so that the quantity $\mathbb{H}(1+\varepsilon)p - \mathbb{H}(p) - \delta$ is equal to some (absolute) negative (constant), say $-\beta$, where $\beta > 0$. Then, $\tau \leq n 2^{-\beta n + 1}$. And choosing $n$ large enough, we can make $\tau$ smaller than $\gamma/2$, as desired. As such, we just proved that
\[
\tau = \mathbb{P}\left[ r \notin S_i \mid r \in R(Y_i) \right] \leq \frac{\gamma}{2}.
\]

Lemma 29.2.2. We have, that $\sum_{r \notin R(Y_i)} w(Y_i, r) \leq \gamma/8$, where $\gamma$ is the parameter of Theorem 29.1.3.

Proof: This quantity, is the probability of sending $Y_i$ when every bit is flipped with probability $p$, and receiving a string $r$ such that more than $\varepsilon p n$ bits where flipped. But this quantity can be bounded using the Chernoff inequality. Let $Z = \Delta(Y_i, r)$, and observe that $\mathbb{E}[Z] = p n$, and it is the sum of $n$ independent indicator variables. As such
\[
\sum_{r \notin R(Y_i)} w(Y_i, r) = \mathbb{P}[|Z - \mathbb{E}[Z]| > \varepsilon p n] \leq 2 \exp \left( -\frac{\varepsilon^2}{4} p n \right) < \frac{\gamma}{4},
\]
since $\varepsilon$ is a constant, and for $n$ sufficiently large. \hfill \blacksquare
Lemma 29.2.3. For any $i$, we have $\mu = \mathbb{E}[W_i] \leq \gamma/4$, where $\gamma$ is the parameter of Theorem 29.1.3.

Proof: By linearity of expectations, we have

$$
\mu = \mathbb{E}[W_i] = \mathbb{E}\left[ \sum_r S_{i,r} w(Y_i, r) \right] = \sum_r \mathbb{E}\left[ S_{i,r} w(Y_i, r) \right]
$$

since $S_{i,r}$ is an indicator variable. Setting, $\tau = \mathbb{P}\left[ r \not\in S_i \mid r \in R(Y_i) \right]$ and since $\sum_r w(Y_i, r) = 1$, we get

$$
\mu = \sum_{r \in R(Y_i)} \mathbb{P}[x \not\in S_i | r \in R(Y_i)] w(Y_i, r) + \sum_{r \not\in R(Y_i)} \mathbb{P}[x \not\in S_i | r \in R(Y_i)] w(Y_i, r)
$$

$$
= \sum_{r \in R(Y_i)} \tau \cdot w(Y_i, r) + \sum_{r \not\in R(Y_i)} w(Y_i, r) \leq \tau + \sum_{r \not\in R(Y_i)} w(Y_i, r) \leq \frac{\gamma}{4} + \frac{\gamma}{4} = \frac{\gamma}{2}.
$$

Now, the receiver got $r$ (when we sent $Y_i$), and it would miss encode it only if (i) $r$ is outside of $R(Y_i)$, or $R(r)$ contains some other codeword $Y_j$ ($j \neq i$) in it. As such,

$$
\tau = \mathbb{P}\left[ r \not\in S_i \mid r \in R(Y_i) \right] \leq \mathbb{P}\left[ Y_j \in R(r), \text{ for any } j \neq i \right] \leq \sum_{j \neq i} \mathbb{P}\left[ Y_j \in R(r) \right].
$$

Now, we remind the reader that the $Y_j$s are generated by picking each bit randomly and independently, with probability 1/2. As such, we have

$$
\mathbb{P}[Y_j \in R(r)] = \sum_{m=1-(1+\varepsilon)n}^{(1+\varepsilon)n} \frac{n^m}{2^n} \leq \frac{n^2}{2^n} \left\langle \frac{n}{1 + (1 + \varepsilon)n} \right\rangle \leq \frac{n^2}{2^n} 2^n (1 + (1 + \varepsilon)n) = n^2 (1 + (1 + \varepsilon)n).
$$

since $(1 + \varepsilon)n < 1/2$ (for $\varepsilon$ sufficiently small), and as such the last binomial coefficient in this summation is the largest. By Corollary 29.3.2 (i), we have

$$
\mathbb{P}[Y_j \in R(r)] \leq \frac{n^2}{2^n} \left\langle \frac{n}{1 + (1 + \varepsilon)n} \right\rangle \leq \frac{n^2}{2^n} 2^n (1 + (1 + \varepsilon)n) = n^2 (1 + (1 + \varepsilon)n).
$$

As such, we have

$$
\tau = \mathbb{P}\left[ r \not\in S_i \mid r \in R(Y_i) \right] \leq \sum_{j \neq i} \mathbb{P}[Y_j \in R(r)] \leq \mathbb{P}[Y_1 \in R(r)] \leq 2^{k+1} n^2 (1 + (1 + \varepsilon)n)
$$

$$
\leq n^2 (1 - \mathbb{H}(p) - \delta + 1 + n \mathbb{H}(1 + \varepsilon)) \leq n^2 \left( \mathbb{H}(1 + \varepsilon) - \mathbb{H}(p) - \delta \right) + 1
$$

since $k \leq n(1 - \mathbb{H}(p) - \delta)$. Now, we choose $\varepsilon$ to be a small enough constant, so that the quantity $\mathbb{H}(1 + \varepsilon) - \mathbb{H}(p) - \delta$ is negative (constant). Then, choosing $n$ large enough, we can make $\tau$ smaller than $\gamma/2$, as desired. As such, we just proved that

$$
\tau = \mathbb{P}\left[ r \not\in S_i \mid r \in R(Y_i) \right] \leq \frac{\gamma}{2}.
$$
In the following, we need the following trivial (but surprisingly deep) observation.

**Observation 29.2.4.** For a random variable \( X \), if \( \mathbb{E}[X] \leq \psi \), then there exists an event in the probability space, that assigns \( X \) a value \( \leq \mu \).

This holds, since \( \mathbb{E}[X] \) is just the average of \( X \) over the probability space. As such, there must be an event in the universe where the value of \( X \) does not exceed its average value.

The above observation is one of the main tools in a powerful technique to proving various claims in mathematics, known as the **probabilistic method**.

**Lemma 29.2.5.** For the codewords \( X_0, \ldots, X_K \), the probability of failure in recovering them when sending them over the noisy channel is at most \( \gamma \).

**Proof:** We just proved that when using \( Y_0, \ldots, Y_{\tilde{K}} \), the expected probability of failure when sending \( Y_i \), is \( \mathbb{E}[W_i] \leq \gamma_2 \), where \( \tilde{K} = 2^{k+1} - 1 \). As such, the expected total probability of failure is

\[
\mathbb{E} \left[ \sum_{i=0}^{\tilde{K}} W_i \right] = \sum_{i=0}^{\tilde{K}} \mathbb{E}[W_i] \leq \frac{\gamma}{2} 2^{k+1} = \gamma 2^k,
\]

by Lemma 29.2.3 (here we are using the facts that all the random variables we have are symmetric and behave in the same way). As such, by Observation 29.2.4, there exist a choice of \( Y_i \)'s, such that

\[
\sum_{i=0}^{\tilde{K}} W_i \leq 2^k \gamma.
\]

Now, we use a similar argument used in proving Markov’s inequality. Indeed, the \( W_i \) are always positive, and it can not be that \( 2^k \) of them have value larger than \( \gamma \), because in the summation, we will get that

\[
\sum_{i=0}^{\tilde{K}} W_i > 2^k \gamma.
\]

Which is a contradiction. As such, there are \( 2^k \) codewords with failure probability smaller than \( \gamma \). We set our \( 2^k \) codeword to be these words. Since we picked only a subset of the codewords for our code, the probability of failure for each codeword shrinks, and is at most \( \gamma \).

**Lemma 29.2.5** concludes the proof of the constructive part of Shannon’s theorem.

### 29.2.2. Lower bound on the message size

We omit the proof of this part.
29.3. From previous lectures

Lemma 29.3.1. Suppose that \( nq \) is integer in the range \([0,n]\). Then \( \frac{2^{n\mathbb{H}(q)}}{n+1} \leq \binom{n}{\lfloor nq \rfloor} \leq 2^{n\mathbb{H}(q)}. \)

Lemma 29.3.1 can be extended to handle non-integer values of \( q \). This is straightforward, and we omit the easy details.

Corollary 29.3.2. We have:

(i) \( q \in [0,1/2] \Rightarrow \binom{n}{\lfloor nq \rfloor} \leq 2^{n\mathbb{H}(q)}. \)  
(ii) \( q \in [1/2,1] \Rightarrow \binom{n}{\lfloor nq \rfloor} \leq 2^{n\mathbb{H}(q)}. \)  
(iii) \( q \in [1/2,1] \Rightarrow \frac{2^{n\mathbb{H}(q)}}{n+1} \leq \binom{n}{\lfloor nq \rfloor}. \)  
(iv) \( q \in [0,1/2] \Rightarrow \frac{2^{n\mathbb{H}(q)}}{n+1} \leq \binom{n}{\lfloor nq \rfloor}. \)

Theorem 29.3.3. Suppose that the value of a random variable \( X \) is chosen uniformly at random from the integers \( \{0,\ldots,m-1\} \). Then there is an extraction function for \( X \) that outputs on average at least \( \lfloor \lg m \rfloor - 1 = \lfloor \mathbb{H}(X) \rfloor - 1 \) independent and unbiased bits.

29.4. Bibliographical Notes

The presentation here follows [MU05, Sec. 9.1-Sec 9.3].

Bibliography