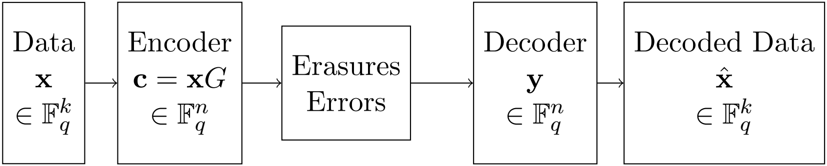
Coding Theory: Errors and Decoding

A Generic Communication Channel

Transmitter

Channel

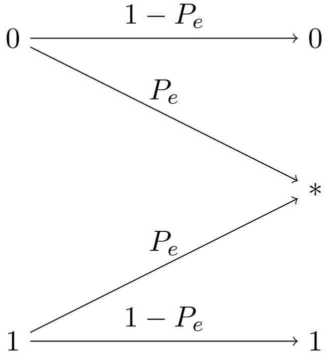
Receiver



$d_H(\mathcal{C}) = d$ means $\mathcal{C}$ can recover from $d-1$ erasures.

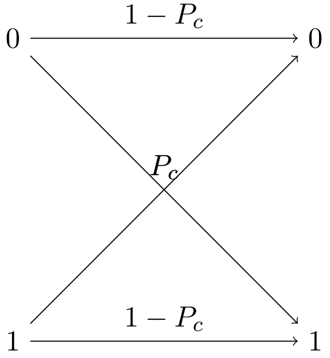
Binary Erasure Channel

Channel with erasure probability P_e, binary input 0 and 1, and ternary output 0, 1 or $*$.



Binary Symmetric Channel

Channel with crossover probability P_c, binary input 0 and 1, and binary output 0 and 1. We assume $P_c < 1/2$.



For $\mathbf{c} \in \mathbb{F}_2^n$:

$P(\mathbf{c}|\mathbf{y})$ = probability that $\mathbf{c}$ is sent given that $\mathbf{y}$ is received.

$P(\mathbf{y}|\mathbf{c})$ = probability that $\mathbf{y}$ is received given that $\mathbf{c}$ is sent.

$P(\mathbf{c})$ = probability that $\mathbf{c}$ is sent.

$P(\mathbf{y})$ = probability that $\mathbf{y}$ is received.

$$P(\mathbf{c}|\mathbf{y}) = \frac{P(\mathbf{c} \cap \mathbf{y})}{P(\mathbf{y})} = \frac{P(\mathbf{y} \cap \mathbf{c})}{P(\mathbf{y})} = \frac{P(\mathbf{y}|\mathbf{c})P(\mathbf{c})}{P(\mathbf{y})}$$

MAP decoder

$$\hat{\mathbf{c}} = \arg\max_{\mathbf{c}\in\mathcal{C}} P(\mathbf{c}|\mathbf{y}),$$

maximum a posteriori probability decoder.

Choose $\hat{\mathbf{c}} = \mathbf{c}$ for the codeword $\mathbf{c}$ with $P(\mathbf{c}|\mathbf{y})$ maximum.

$P(\mathbf{c}|\mathbf{y}) = \frac{P(\mathbf{y}|\mathbf{c})P(\mathbf{c})}{P(\mathbf{y})}$.

ML decoder

$$\hat{\mathbf{c}} = \arg\max_{\mathbf{c}\in\mathcal{C}} P(\mathbf{y}|\mathbf{c}),$$

maximum likelihood decoder.

Choose $\hat{\mathbf{c}} = \mathbf{c}$ for the codeword $\mathbf{c}$ with $P(\mathbf{y}|\mathbf{c})$ maximum.

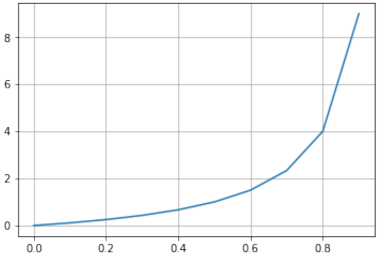
$$P(\mathbf{c}|\mathbf{y}) = \frac{P(\mathbf{y}|\mathbf{c})\,P(\mathbf{c})}{P(\mathbf{y})}.$$

For $\mathbf{c} = (c_1, \ldots, c_n)$ sent over a binary symmetric channel:

$$
\begin{aligned}
P(\mathbf{y}|\mathbf{c}) &= \prod_{i=1}^{n} P(y_i|c_i) \text{ (bit errors are independent)} \\
&= P_c^{d_H(\mathbf{y},\mathbf{c})}(1-P_c)^{n-d_H(\mathbf{y},\mathbf{c})} \\
&= (1-P_c)^n \left(\frac{P_c}{1-P_c}\right)^{d_H(\mathbf{y},\mathbf{c})}
\end{aligned}
$$

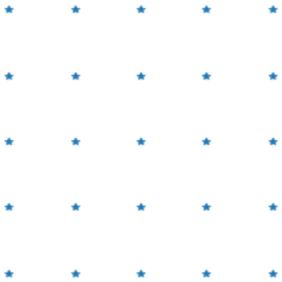
$$P(\mathbf{y}|\mathbf{c}) = (1 - P_c)^n \left(\frac{P_c}{1-P_c}\right)^{d_H(\mathbf{y},\mathbf{c})}$$

For $P_c < 1/2$, $P_c/(1 - P_c) < 1$.
Maximize $P(\mathbf{y}|\mathbf{c}) \iff$ minimize $d_H(\mathbf{y}, \mathbf{c})$.
Decode the codeword closest to the received vector.



Decoding

■ Maximum likelihood



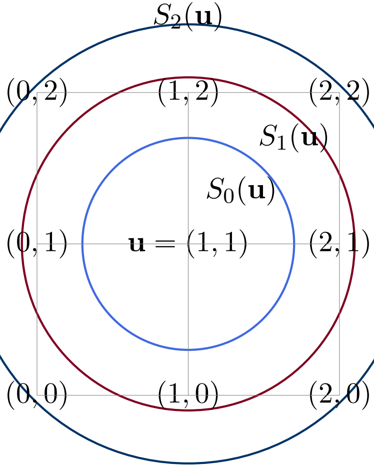
$\mathbf{y} = \mathbf{c} + \mathbf{e} \iff \mathbf{e} = \mathbf{y} - \mathbf{c} \iff \mathbf{c} = \mathbf{y} - \mathbf{e}$ (the noise maps a vector to another vector).

Noise adds an error vector $\mathbf{e}$ to $\mathbf{c}$, the goal of decoding is to determine $\mathbf{e}$.

Nearest neighbour decoding finds a vector $\mathbf{e}$ (which may not be unique) of smallest weight such that $\mathbf{y} - \mathbf{e}$ is in the code. [Maximize $P(\mathbf{y}|\mathbf{c}) \iff$ minimize $d_H(\mathbf{y}, \mathbf{c})$.]

Hamming spheres

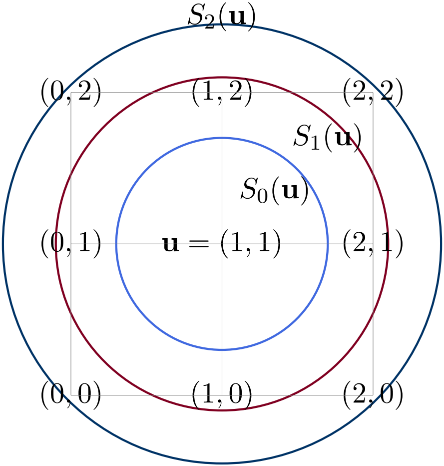
$S_r(\mathbf{u}) = \{\mathbf{v} \in \mathbb{F}_q^n,\ d_H(\mathbf{u},\mathbf{v}) \le r\}$



Hamming spheres

$|S_r(\mathbf{u})| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$

$$|S_0(\mathbf{u})| = 1,$$
$$|S_1(\mathbf{u})| = 5,$$
$$|S_2(\mathbf{u})| = 9.$$



Hamming spheres

$|S_r(\mathbf{u})| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$.

At distance r, a vector is distinct in r coordinates. There are $\binom{n}{r}$ ways to choose these coordinates, and in each position there are $q-1$ choices of values (any element in $\mathbb{F}_q$ but the one already in $\mathbf{u}$).

Hamming spheres

If $d_H(\mathcal{C}) = d$, and $t = \lfloor \frac{d-1}{2} \rfloor$, then spheres of radius t around distinct codewords are disjoint.

If $\mathbf{v} \in S_t(\mathbf{c}_1) \cap S_t(\mathbf{c}_2)$, then by the triangle inequality:

$$\begin{aligned} & d_H(\mathbf{c}_1, \mathbf{c}_2) \\ \leq \quad & d_H(\mathbf{c}_1, \mathbf{v}) + d_H(\mathbf{v}, \mathbf{c}_2) \\ \leq \quad & 2t < d \end{aligned}$$

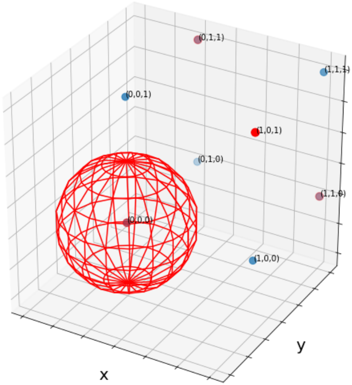
implying $\mathbf{c}_1 = \mathbf{c}_2$.

Decoding

Hamming spheres

Error correction

Nearest neighbour decoding uniquely and correctly decodes any received codeword in which at most t errors have occurred.



maximimum likelihood decoding

Hamming spheres

Connection to error correction