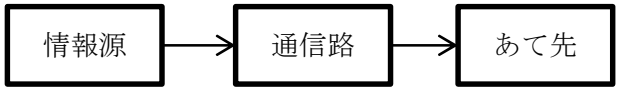
情報理論 第１回　情報と情報量

1. 情報理論とは

- 情報を系統的に(数学的に)扱う理論のこと
  - 情報の保存・伝達・保護を効率的に行うのに役立つ

2. 情報伝達

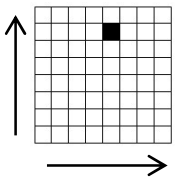
- 単純に情報をそのまま伝える
  - 模式的に表すと



  - 効率が悪い
  - だれかに情報を盗み見られる可能性がある
  - 情報が伝達中に狂っても修正できない

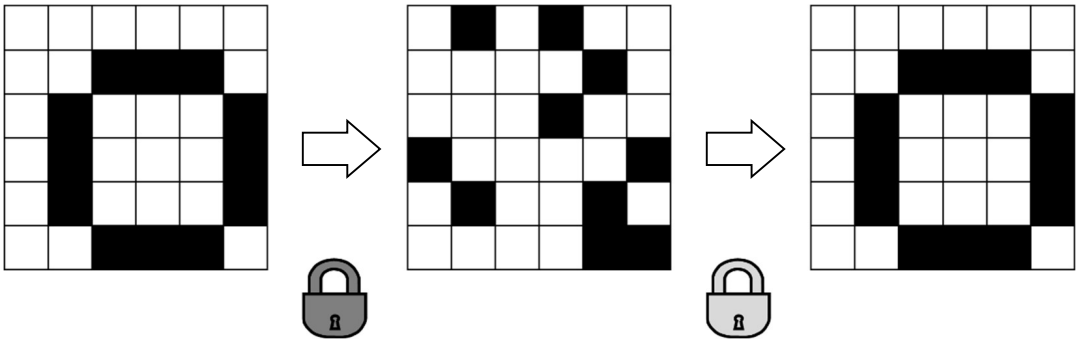
- これを改良するための工夫
  - 効率よく伝達・記憶する　→　**圧縮**
  - 第三者に見られないようにする　→　**暗号化**
  - 誤りをできるだけ少なくする　→　**誤り訂正**

- 圧縮
  - なるべく少ない信号で情報を伝えたい
  - 例：8×8 のマスに 1 つだけ点があることがわかっているときに、その点がどこにあるかを伝える



    - 方法 1：あいているマスを 0, 黒いマスを 1 として、下の行から順に「0000…000100…」のように送る→信号の数は 64
    - 方法 2：横方向の情報を「00001000」、縦方向の情報を「00000010」のようにして送る→信号の数は 16 (これは受け取る側が「全体が 8×8 の構造になっていること」を知っている前提のもとで使える方法)
    - 方法 3: 横方向の情報を「100」、縦方向の情報を「110」のようにして送る→信号の数は 6 (これは受け取る側が「全体が 8×8 の構造になっていること」「黒いのは 1 か所だけであること」を知っている前提のもとで使える方法)
  - 工夫するほど信号の数は減らせる
    - **最小でどこまで減らせるか　→　情報理論で数値がわかる**

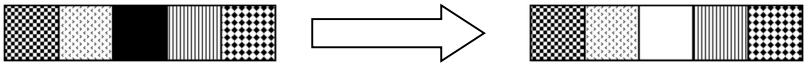
- 暗号化
  - 伝送中に第三者に見られても情報が漏れないようにしたい



  - 「鍵」を使って情報のかたちを変える
    - ✧ 送る側：「暗号化の鍵」を使う
    - ✧ 受け取る側：「復号化の鍵」を使う
  - 伝送中の信号を見ても、中央の図のようなものしかわからない
  - 「復号化の鍵」がわかりにくいほど、情報は安全になる(RSA 暗号、量子暗号…)

- 誤り訂正
  - 伝送の途中で変化したり、失われた情報を回復したい

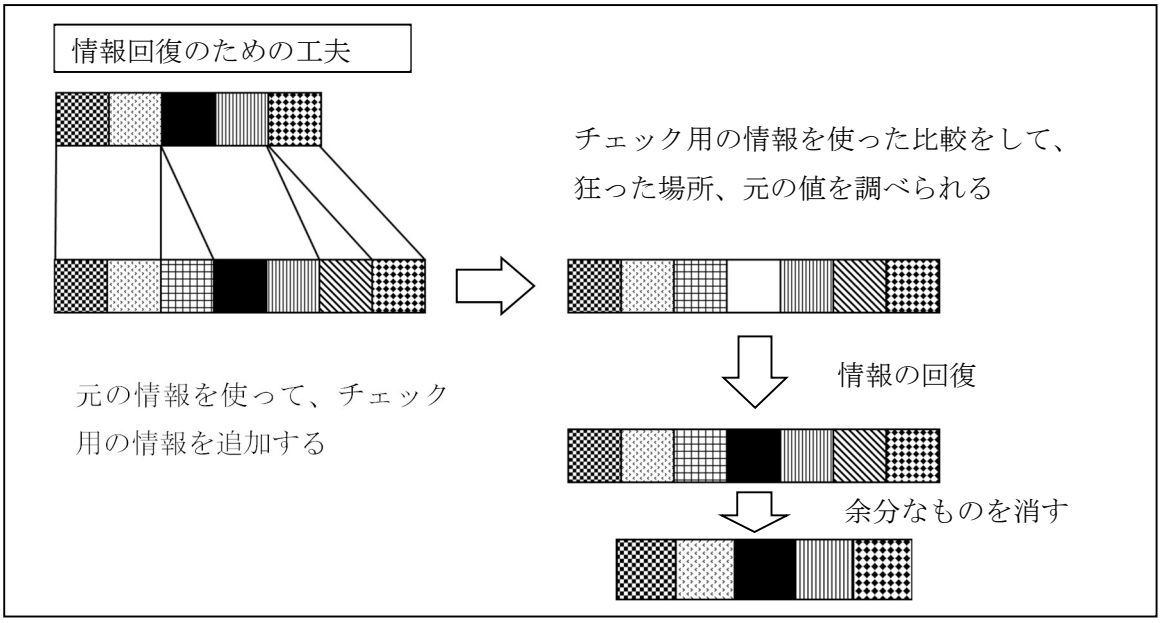
そのまま送ると



途中で情報が狂うかもしれない

あて先(受け取った側)では
- ✧ 狂ったかどうか
- ✧ どこが狂ったか
- ✧ 元の値は何か

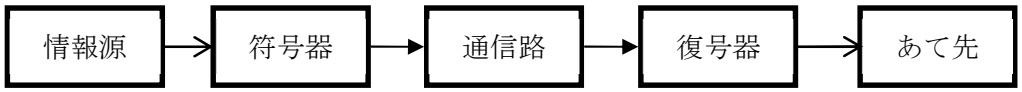
がわからない



- チェック用の情報をたくさん追加すると
  - ✧　伝送中の信号の変化が多くても対処できる
  - ✧　でも、信号はその分長くなる
- 情報をどのくらい追加すると戻せる確率はどれくらいになるか　→　情報理論で数値がわかる

3. 現代の情報伝達

- 情報伝達の模式図(改良版)



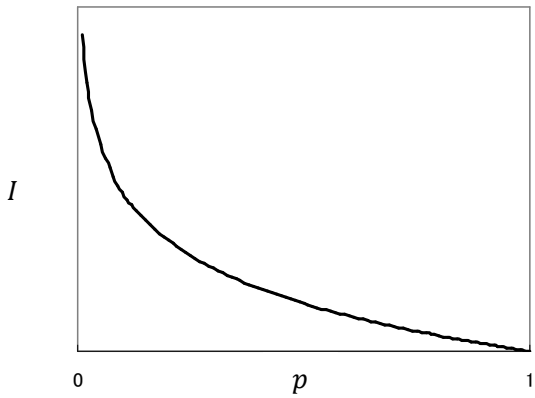
- 情報源(情報を送る人)
  - 符号器：圧縮・暗号化・誤り訂正の符号追加の順に処理をする
  - この３つの処理をまとめて**符号化**という
- あて先(情報を受け取る人)
  - 復号器：誤り訂正と余分な符号の削除・暗号の復号化・解凍の順に処理をする
  - この３つの処理をまとめて復号化という

※ 符号器
- 情報源符号器：生のデータを効率の良い 0, 1 の情報に変える(圧縮)
- 暗号器：情報を暗号化する
- 通信路符号器：誤りを元に戻すためのデータを加える

※ 復号器
- 通信路復号器：誤り訂正と、余分な符号の削除をする
- 暗号の復号器：暗号から元の情報を取り出す
- 情報源復号器：0, 1 の情報を元の形に翻訳する

4. 情報量とは

- 情報量：情報の多さを数値で表わしたもの
  - 例：「サイコロを振って 3 の目が出た」「コインを投げて表が出た」という情報も、明確に数値で表わせる
- 確率と情報量
  - 情報量は、その出来事のおこる確率が低いほど多い
    - 「サイコロを振って 1 の目が出た」と「サイコロを振って 2 の目が出た」という情報の情報量は同じ(確率はどちらも 1/6)
    - 「サイコロを振って 1 の目が出た(確率は 1/6)」と「サイコロを振って 1～3 のどれかの目が出た(確率は 1/2)」を比べると、前者の方がより詳細な情報→情報量が多い
  - 情報量の組み合わせ
    - 全く関係のない 2 つの出来事を同時にしらせる情報の情報量は、それぞれの出来事の情報の情報量を足したものになる
    - 例：情報量(サイコロを振ってコインを投げたら、サイコロは 1, コインは表が出た)
      = 情報量(サイコロを振ったら 1 が出た) + 情報量(コインを投げたら表が出た)
  - 定義
    - 情報量 I を確率 p の関数で書くと、$I(p) = -log(p)$となる。
  - この定義からわかること
    - $p = 0$では I は無限に大きくなる(起こりにくいことについての情報は情報量が多い)
    - $p = 1$では I は 0 になる(確実に起こることの情報は「無意味」)



※　注意

- $I(p) = -log(p)$と書いたときの対数の底(てい)は 2
  - 対数は一般には$\log_b a$のような形で書く。この場合は b が対数の底
  - 情報理論で対数の底が省略されているときは、底は 2

5. 対数の性質

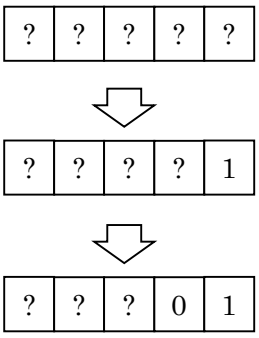
- 対数の数学的なルール

1.	$\log_b 1 = 0$
2.	$\log_b b = 1$
3.	$\log_b a^c = c \log_b a$
4.	$\log_b a = \frac{\log_c a}{\log_c b}$
5.	$\log_b(cd) = \log_b c + \log_b d$

a, b, c, d は任意の正の数

- これらのルールからわかること
  - 確実に起こること(起こる確率が 100% = 1)についての情報量
    $I(1) = -\log_2 1 = 0$ (ルール 1)
  - 起こる確率が 50% = 0.5 の出来事の結果を伝える情報の情報量
    $I(0.5) = -\log_2 0.5 = -\log_2(2^{-1})$
    ここでルール 3 を使うと
    $I(0.5) = -(-1)\log_2 2 = \log_2 2$
    さらにルール 2 から
    $I(0.5) = 1$
    がわかる。

ところで、普通のデジタル信号は 0, 1 のつながりで表わされる。



信号を受け取る前はまだ何も情報がない

「一つ分」信号を受け取ると、0, 1 のどちらかわからなかったことが確定
→確率 50%のことについての情報が得られる→**情報量が 1 増える**

もう一つ信号を受け取ると、さらに**情報量が 1 増える**

「2 進数で何ケタ分」という感覚でよく使われる「bit」は、情報量の単位でもある。確率が 1/2 や 1/4 などの出来事だと情報量は整数になるが、たとえば確率 1/3 の出来事だと$I(1/3) = \log_2 3 = 1.58\ldots$のように半端な値になる。

練習問題

次の出来事に関する情報量を求めよ。ただし$\log_2 3 = 1.58$とし、計算結果は四捨五入して小数第二位までにすること。

(1) コインを 3 枚投げ、すべて表になった。
(2) コインを 3 枚投げ、2 枚が表、1 枚が裏になった。
(3) 六面体の(普通の)サイコロを振り、2 以下の目が出た。
(4) 八面体のサイコロを振り、1 の目が出た。
(5) 八面体のサイコロを振り、6 以下の目が出た。