高知大学　秋の公開講座
ユビキタス情報社会を支えるソフトウェアの世界

第4回
安全・確実に情報を伝える

高知大学 理学部 数理情報科学科
塩 田 研 一
mail: shiota@is.kochi-u.ac.jp
http://lupus.is.kochi-u.ac.jp/~shiota/

2005年9月29日

講師の専門分野

- 保型形式の整数論
  - フェルマー予想解決の道具となった整数論の中心分野
  - 博士論文では50年間未解決だった問題を解決
- 計算代数
  - 代数/整数計算を行うアルゴリズム・プログラムの開発
- 誤り訂正符号
- 暗号理論
- 組合せ論・グラフ理論
- 民俗学

Q & A

ご質問、ご意見ありましたら

今日のお話

1. 信号とは
2. 通信の歴史
3. デジタル信号の利点
4. デジタル信号の誤りを自動的に訂正する技術
5. アナログ情報をデジタル信号に変換する方法
6. 暗号の必要性
7. 昔から使われてきた暗号
8. インターネット時代の新しい暗号：公開鍵暗号
9. 暗号技術の色々

まずは通信の歴史を振り返りましょう

信号とは
― 音の届かない距離で情報を伝達する方法 ―

- のろし
  … 光を利用、伝えられる情報は1つだけ
- 手旗信号
  … 光を利用、文字を真似たパターン
- モールス信号
  … 電信用、トン・ツーの組合せで文字を表現

電信の始まりはデジタル

- 1835年： パルス送信に成功
- 1837年： 最初の電信会社設立
- 1844年： モールス信号による公開実験成功
- 1848年： テレプリンタ使用開始
- 1851年： 電信会社が営業開始

音も送りたい

- 解剖学的に
  音 → 鼓膜が振動 → 知覚
- だったら
  膜を振動 → 音が再現 ？
- 1860年： ライスが電流から音を再生
- 1876年： ベル・グレイ・エジソンらが電話を発明
- 1877年： エジソンが蓄音機を発明

無線通信の始まり

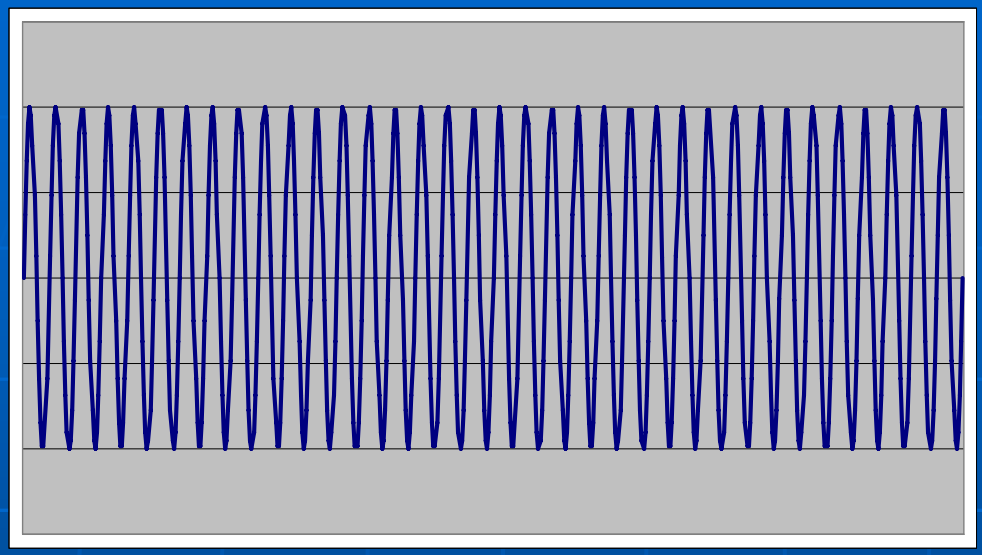
- 1864年：　電磁波の理論的存在証明
- 1888年：　電磁波存在の実証
- 1894年：　無線電信実験成功
- 1897年：　無線電信会社設立

アナログ無線通信へ

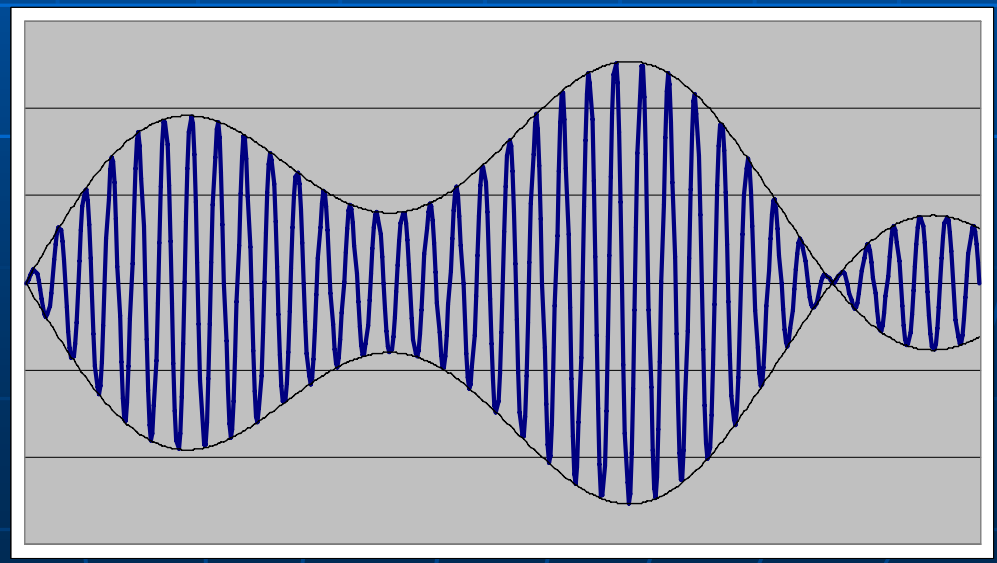
- 1906年: 鉱石検波器の発明
- 1906年: 無線電話の実験
- 1920年: 民間放送開始
- 1933年: FM方式の発明
- 1961年: FMステレオ放送開始

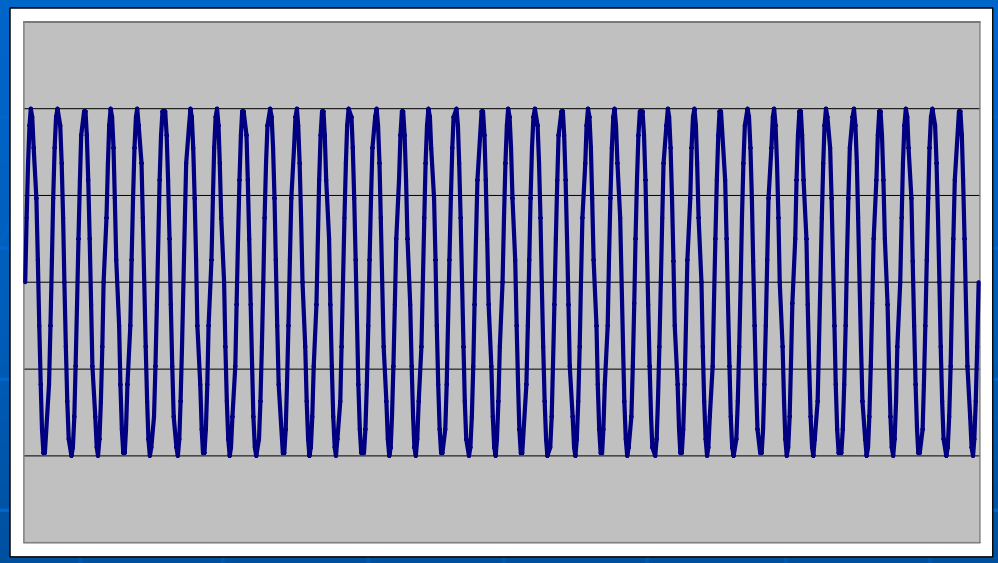
AM と FM

- AM = Amplitude Modulation
  （振幅変調）
  … 搬送波の振幅のずれで信号を表現
- FM = Frequency Modulation
  （周波数変調）
  … 搬送波の周波数のずれで信号を表現

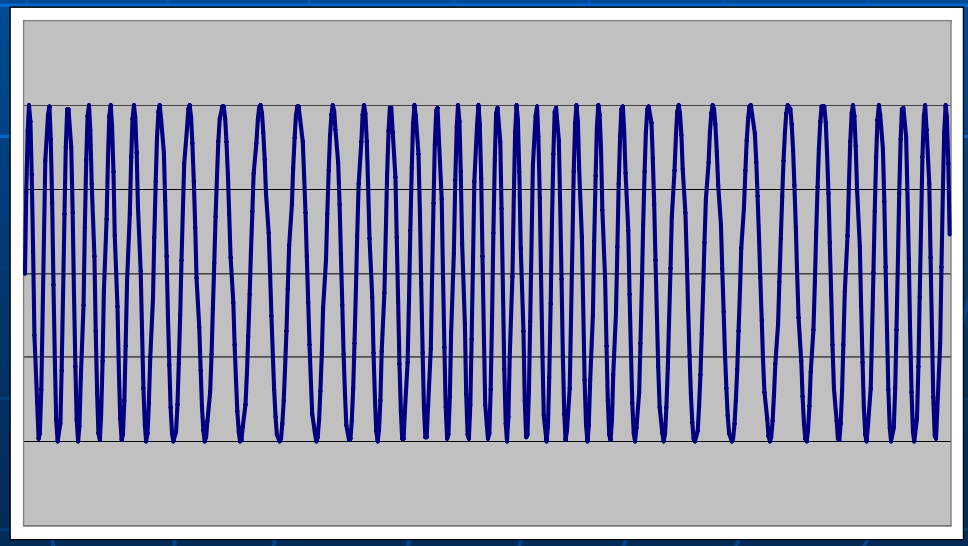


AM





FM



Q & A

ご質問、ご意見ありましたら

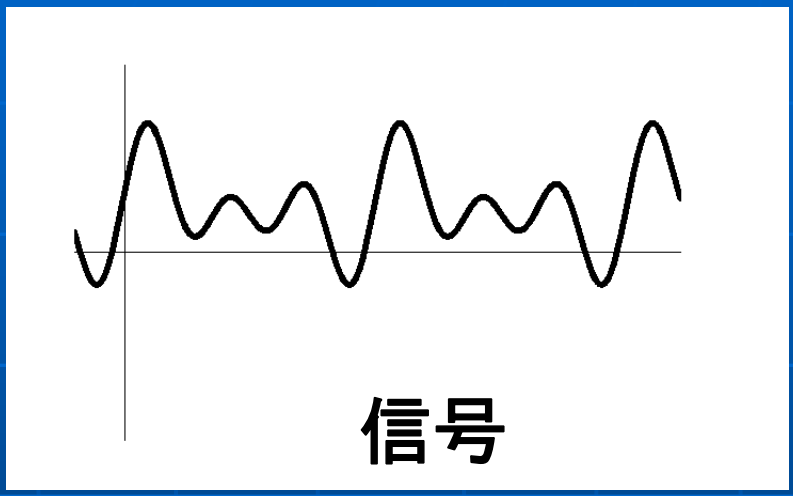
歴史的に

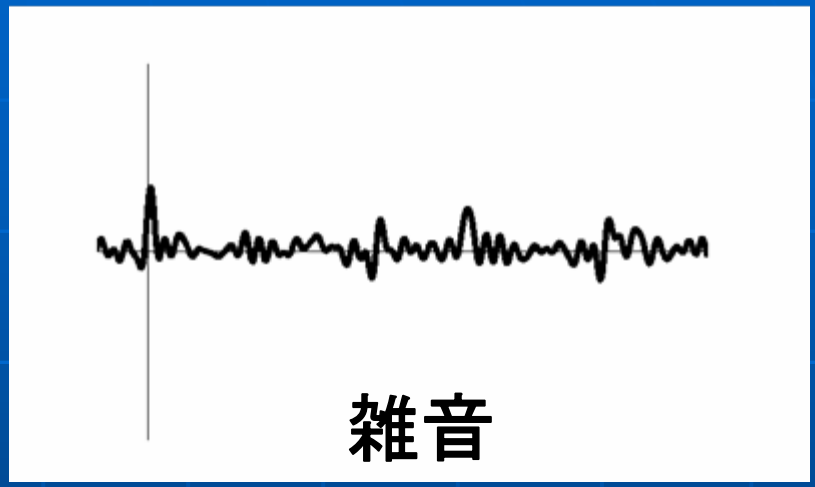
- 通信はデジタルで始まった
- 技術の発達によってアナログ通信が可能に
- しかし、今またデジタルの時代

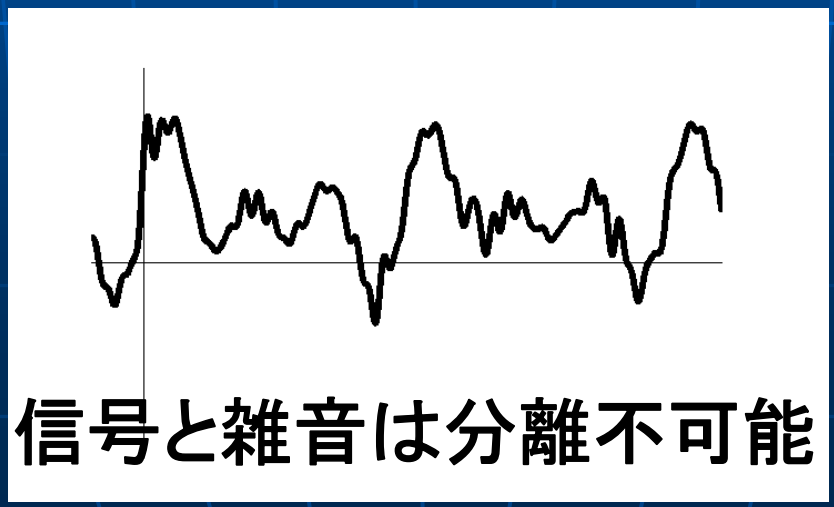
… なぜ？

次はデジタル信号のお話です

アナログの宿命 … 雑音は免れない

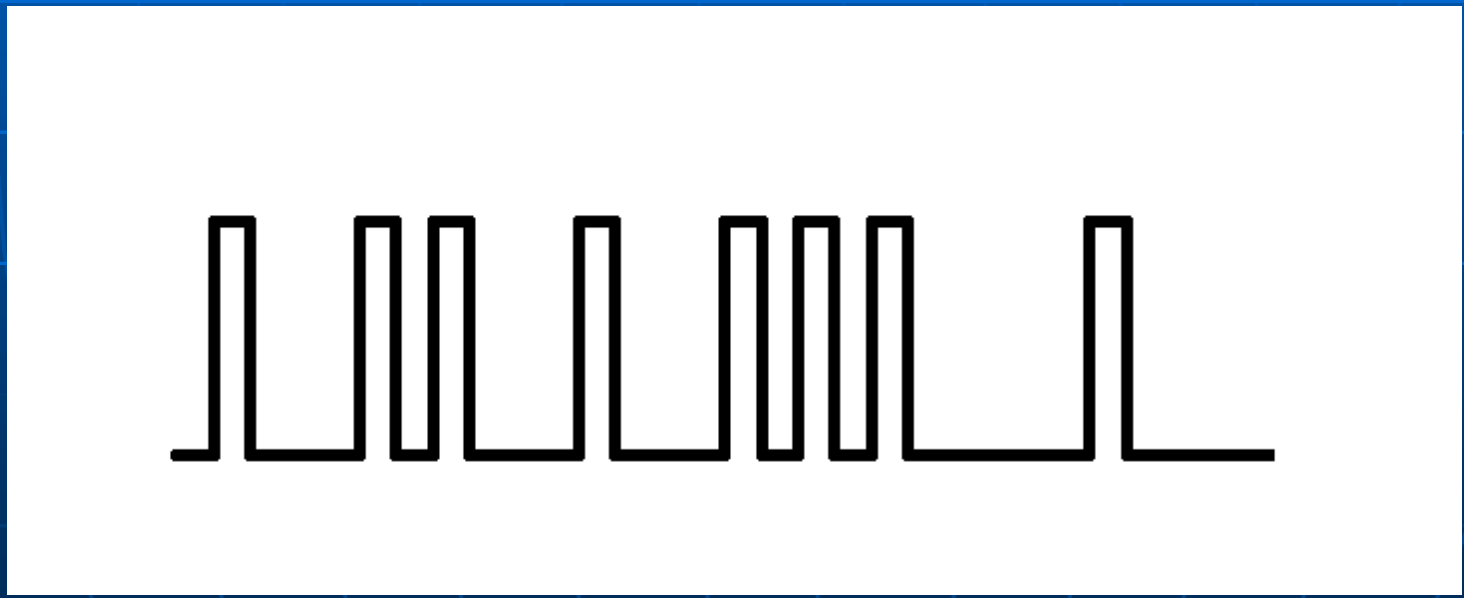




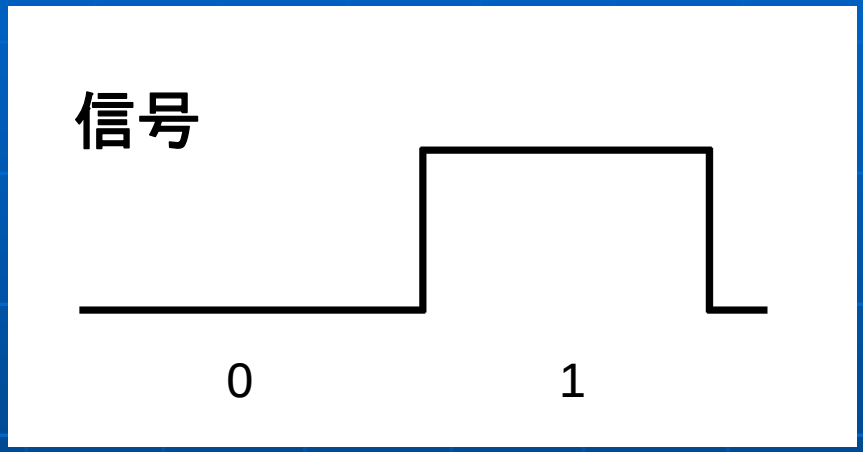


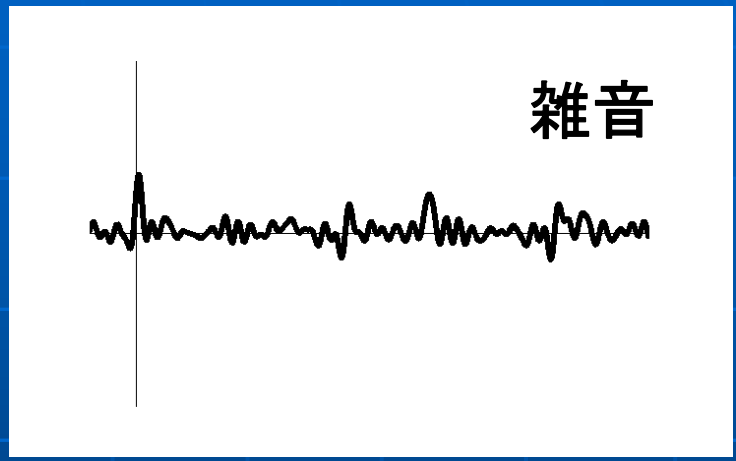
デジタル信号とは

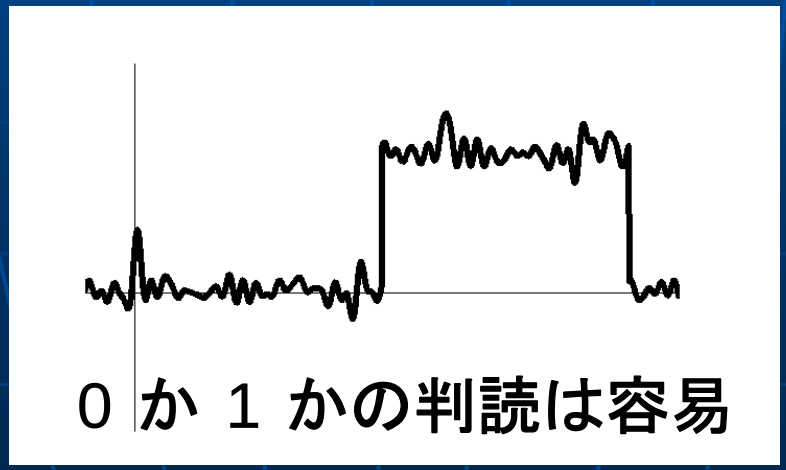
０　または　１　を一定間隔で並べた信号



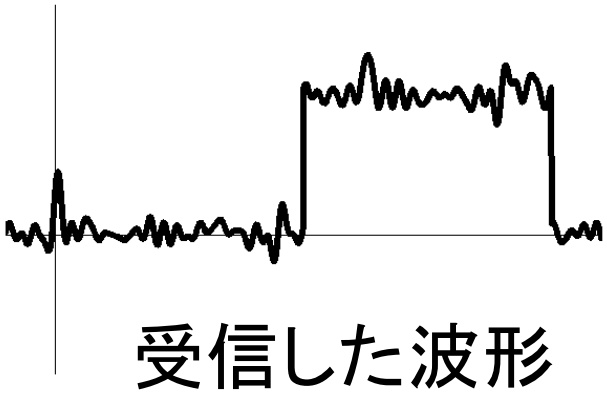
デジタル信号が雑音に強い理由 1







デジタル信号が雑音に強い理由 2



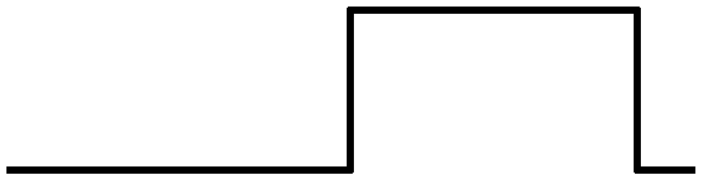
受信した波形

中継点で

完全な0か1

に復元して次へ送信

すればOK

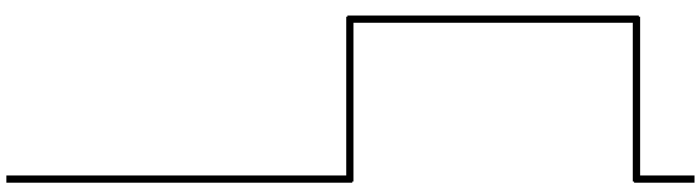


綺麗に復元してから送信

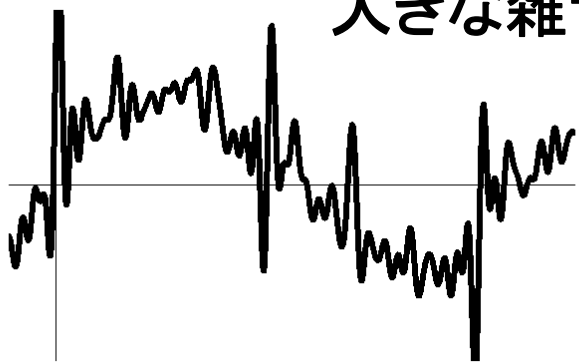
それでも誤りは起こる

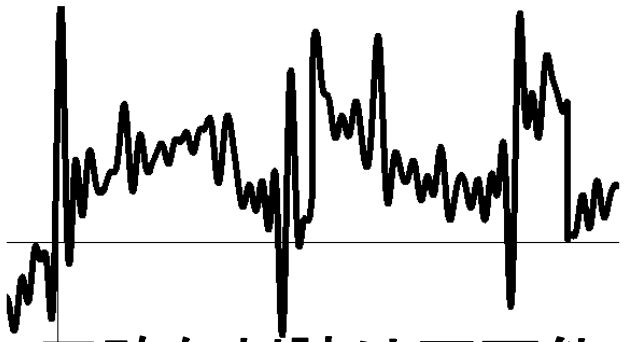
- 0 か 1 かの判定
  … 0.5 より大きいか小さいか
- 雑音が大きくて 0.5 以上狂えば、やはり判定ミスが …

信号



大きな雑音





正確な判読は不可能

ここで誤り訂正技術が登場します

デジタル信号が雑音に強い理由 3

- 信号の作り方を工夫すると …
  ある程度の判定ミスが自動的に訂正可能
- 工夫とは …
  - 0,1 を幾つかまとめてブロックにする
  - 各ブロックに「おまけ」を付ける
  - 「おまけ」の効果で
    - 判定ミスを検出
    - 正しい信号に復元

簡単な例

- ブロック = 1 ビット (0 か 1 かのひとつ分)
- おまけ = 更に 2 つ !!
- つまり
  - 0 → 000 にして送信
  - 1 → 111 にして送信

- 例えば、100 を受信したら誤りが起こったことがわかる

信号の訂正方法

- 正しいパターンは 000 と 111 だけ

  100 と 000 の違い: 1 ビット
  100 と 111 の違い: 2 ビット

  ⇒ 100 は 000 の間違い、と考えるべき

- つまり 100 は 000 に訂正しよう

- 同じく

  010, 001 は 000 に訂正しよう
  011, 101, 110 は 111 に訂正しよう

このように

信号に「おまけ」を付けて誤りを自動訂正する仕組みを

誤り訂正符号

と言う

Q & A

ご質問、ご意見ありましたら

さっきの例は

データ量が3倍になってしまう

もっと上手い方法はないかな？

日常会話に立ち返ると …

- 結婚式でお父さんのスピーチ
  「ふしだらな娘ですが … 」

「ふつつか」と言いたかったのだろう

- 誤り訂正の原則:
  一番似ている、正しいパターンを探せ

ということは

- できるだけ似ていないパターンを
  正しいパターンとして採用せよ
  ⇒「どの正しいパターンに似てるか」
  を考え易い

- 田村早苗（たむらさなえ）さんと
  田浦花江（たうらはなえ）さんが
  同じクラスにいたらややこしいのと一緒

ブロック長 7 のハミング符号

7桁の2進数:
128パターン

うち、右の16パターンを正しい信号に採用
（右3桁がおまけ）

正しい信号同士は
お互い3桁以上違う

0000000	1111111
0111000	1000111
1010100	0101011
1101100	0010011
1100010	0011101
1011010	0100101
0110110	1001001
0001110	1110001

ブロック長 8 のアダマール符号

8桁の2進数:
256パターン

うち、右の16パターンを
正しい信号に採用
（第4,6,7,8 桁がおまけ）

正しい信号同士は
お互い4桁以上違う

00000000	11111111
01010101	10101010
00110011	11001100
01100110	10011001
00001111	11110000
01011010	10100101
00111100	11000011
01101001	10010110

音楽CDの音声信号

- ブロック長 ＝ 24 ビット
- おまけ ＝ 8 ビット
- 合計 ＝ 32 ビット

- ひとつの音の情報が1箇所に固まらないような工夫も

誤り訂正符号に求められる能力

- 訂正能力：訂正できる誤りの割り合い
- 情報率：「おまけ」は少なくしたい
- 処理速度（記録時、再生時）
- 生産コスト
- 機材の重量 etc.

- 全てを満たすのは不可能

⇒　状況に応じて優先順位を

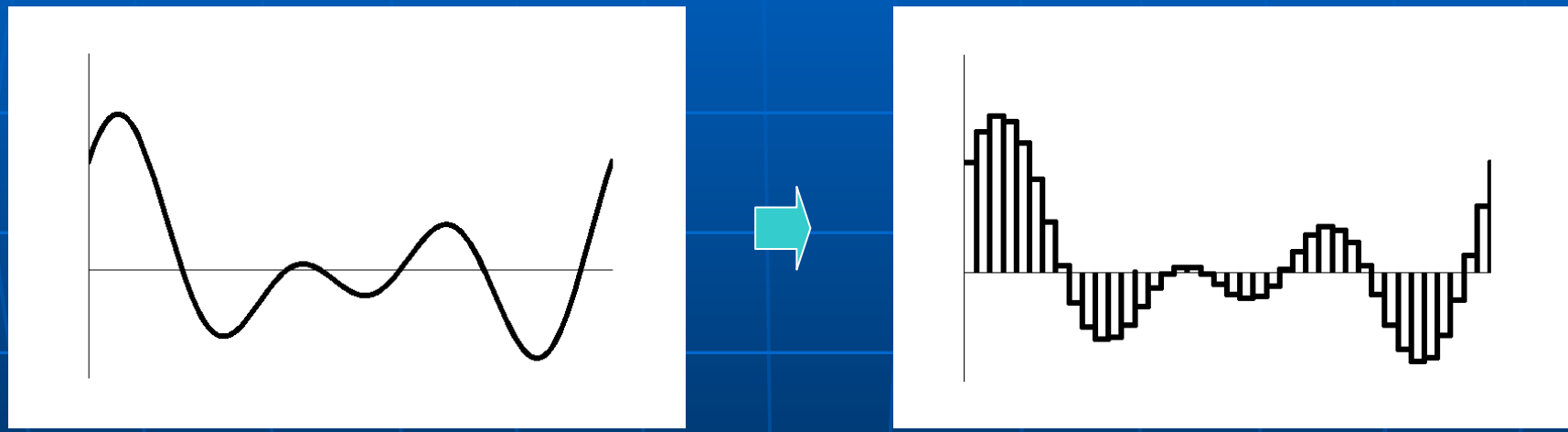
Q & A

ご質問、ご意見ありましたら

ところで、アナログ情報を
デジタル信号に変換する方法は？

アナログ情報をデジタル信号に変換する方法（CDの例）

- 音波の波形を棒グラフに直す:



- 棒の幅：1/44100 秒
- 棒の高さ：65536 段階で表現

  65536通り ＝ 16桁の2進数 ＝ 16ビット

音楽CDの記憶容量

- 生データは
  44100 区画 × 60 秒 × 74 分 ×16 ビット × 右左
  = 約 6.27 × 10^9 ビット = 約 747 MB
- 誤り訂正のおまけを付けて 4/3 倍
- 更に、安定した読取りの為のおまけをつけて 17/8 倍
- 更に更に、タイミングを取る為のおまけもプラス
  ⇒ 結局、生データの 49/16 倍の情報約 2.2 GB

- CD-ROM は更に強い誤り訂正が必要 → 640 MB

アナログ情報をデジタル信号に変換する方法（静止画の例）

- 三原色 = 青，赤，緑
- 液晶画面 = 小さな点（ピクセル）の集まり

- 各ピクセルの色を青，赤，緑色成分に分離
- 各成分の明るさを 256 段階で表現
  （256 通り = 8 ビット）
- このままでは情報量が膨大
  ⇒ 情報圧縮技術の出番

静止画の画像形式

- bmp（ビットマップ）:
  … 情報そのまま
- gif（ジフ）:
  … 使う色の種類を少なく
- jpg（ジェイペグ）:
  … 色の分布を三角関数で大雑把に近似
  - 画質（＝近似誤差の許容度）が指定可能

情報圧縮のアイデア色々

- 出現頻度の高いものは短い名前で
  … モールス信号 etc.
- ディティールを犠牲に
  … jpg　etc.
- 似たもの同士は「差」だけを記録
  … mpeg etc.

中間まとめ

- デジタル信号は雑音に強い
- アナログ情報は棒グラフに直してデジタルに
- デジタル信号に更に「おまけ」を付けると …

「おまけ」の効果で誤りの自動訂正が可能に

Q & A

ご質問、ご意見ありましたら

後半は暗号のお話です

シーザー暗号

- L　ORYH　BRX　って ???

- 実はアルファベットを3文字ずらしたもの
  正解：I　LOVE　YOU

暗号とは

- 読める文章（平文）を読めない文章（暗号文）に変換する方法
- 送信者：平文 x を暗号文 $y = f(x)$ に変換
- 受信者：逆関数を用いて $f^{-1}(y) = x$ を解読
- シーザー暗号では
  - f　：3 文字後ろにずらすこと
  - f^{-1}：3 文字前にずらすこと

1970年頃までの暗号は

- 送信者と受信者が「秘密の関数 f(x)」を共有
- f(x) がバレれば逆関数 $f^{-1}(y)$ もバレる
- 古典暗号、共通鍵暗号、対称暗号などと呼ばれる

1975年 Diffie-Hellman のアイデア

- f(x) がバレれても逆関数 $f^{-1}(y)$ がバレない、そんな関数があれば …
- 暗号文を受け取りたい人は f(x) を公開して自分だけ $f^{-1}(y)$ を使って読めば良い
- 例えば
  - 商店は f(x) を公開
  - お客さんは注文書を f(x) で暗号化して送信

… 安心だよね

このような暗号方式を

公開鍵暗号

と言う

でもそんな都合のいい関数なんてあるの ??

f(x) がわかってれば $f^{-1}(y)$ って計算できるんじゃないの ???

1977年 最初の公開鍵暗号登場

- Rivest, Shamir, Adleman の共同研究
- 整数関数を使って理想的な f(x) を構成
- 3人の頭文字を取って「RSA 暗号」と命名

- その後も次々と新しい暗号方式が
  ElGamal 暗号、楕円曲線暗号　etc.

マジックのタネ

- 高速にできる計算と、天文学的な時間の掛かる計算を上手に利用
- f(x) は高速な計算で
- $f^{-1}(y)$ の計算には時間が掛かるように

例えば

- 問い:

  p = 5025103959178413661189033433113

  と

  q =3815031238347521782706056223475180997

  を掛けあわせなさい

- 答え:

  n = 191709285802094580188990542658097265635287841065727130244119681536 61

  … これは頑張れば手でもできる

ところが

- 問い:

  n =191709285802094580188990542658097265635287841065727130244119681536 61

  を2つの数に分解しなさい

  … これは少々頑張っても無理

公開鍵暗号の使い方

- ひとりひとりが自分の暗号化関数を公開
  （ Aさんの関数 ＝ $f_A(x)$ ）
- $f_A(x)$ を集めた暗号帳を作成
  （ 暗号帳 ： 電話帳のようなもの ）
- 暗号通信をしたい人は暗号帳を引いて関数を使う

インターネット時代では

- ネット上では情報は野ざらし
- 悪人もつなぎ放題

- 暗号通信は必須

ネット人口は6億人を突破

- 6億人が古典暗号で通信しようとすると
  … 18×10^{16} ＝ 18京通りの関数が必要
- 公開鍵暗号なら6億通り
- その比は3億分の１ !!!
- 第一、古典暗号だと変換式　f(x) 自体も暗号で送らないと !!

公開鍵暗号の応用で

次のような技術が実現

- 電子マネー
- 電子投票
- 電子認証
- 通信上のコイントス
- ゼロ知識証明

公開鍵暗号のこれから

- 計算の高速化
- ダウンサイジング
- セキュリティ向上　etc.

暗号のまとめ

- 暗号 ＝ 情報を第3者には読めないように変換すること
- 変換式を公開してしまう公開鍵暗号が誕生
  - インターネット時代では必須の技術
  - 電子マネー、電子認証など応用技術も多彩

Q & A

ご質問、ご意見ありましたら

時間が余ったら音楽の話でも

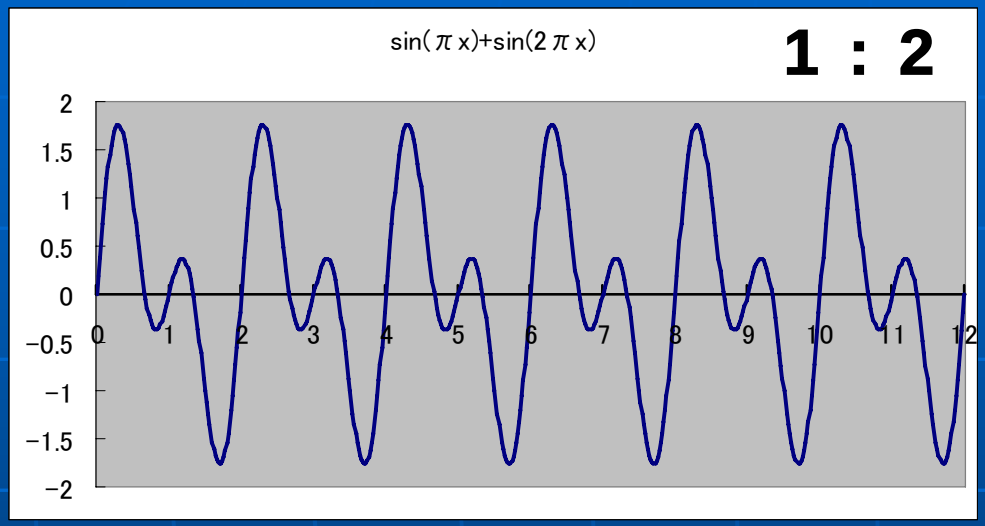
ギターのフレームは

同じ比率で並んでいる

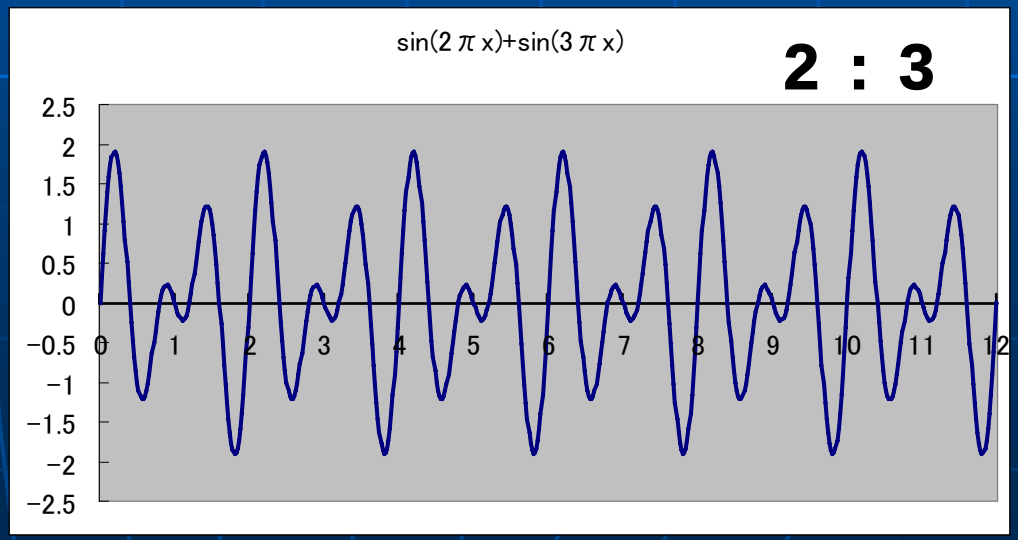
比率 ＝ $2^{(1/12)}$

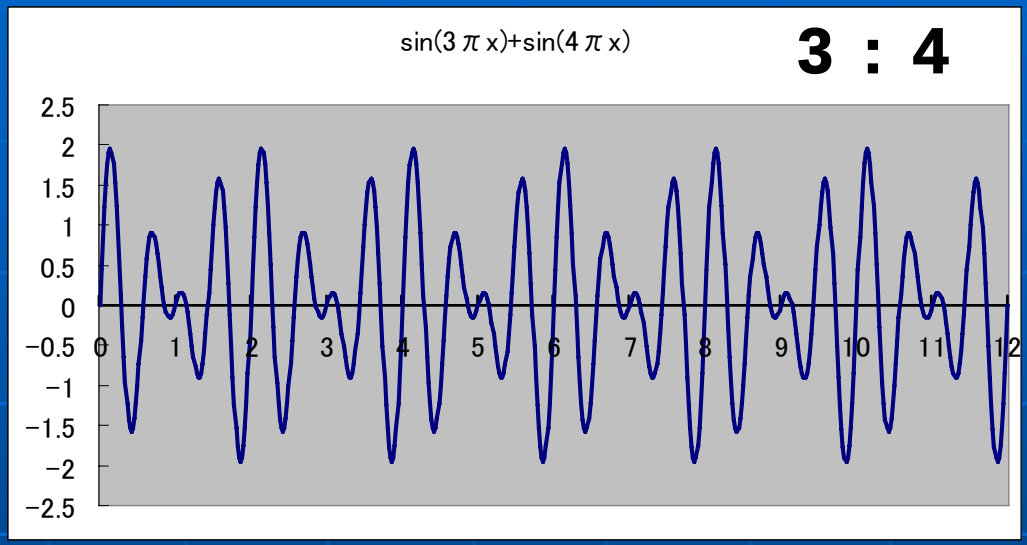
＝ 1.05946…

音がハモる、とは？

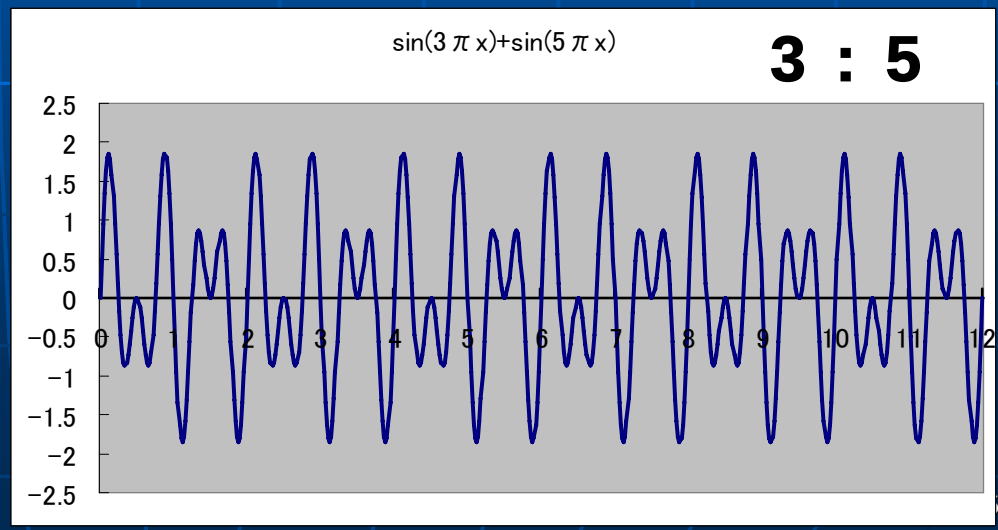


波長・周波数が
単純な整数比
になること

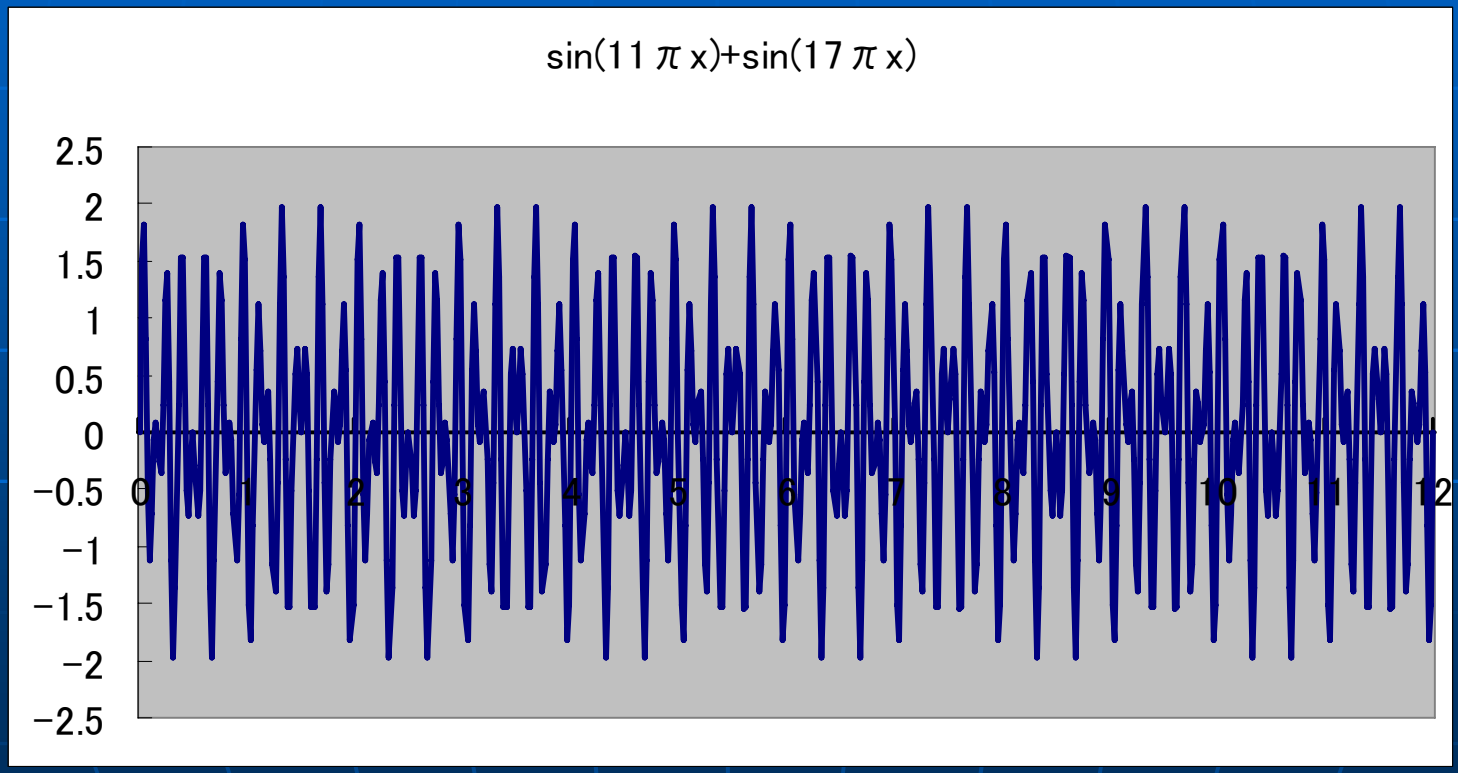




音を重ねても
パターンが単純
⇒　心地よい



ハモっていない場合



1 オクターブ = 12 音　の理由

- $r = 2^{(1/12)} = 1.05946\ldots$ とすると
  - $r^3 = 1.189\ldots \fallingdotseq 6/5$
  - $r^4 = 1.259\ldots \fallingdotseq 5/4$
  - $r^5 = 1.335\ldots \fallingdotseq 4/3$
  - $r^7 = 1.498\ldots \fallingdotseq 3/2$
  - $r^{12} = 2$
- ハモる比が全て r で表される

和音の周波数比

- 長調　ド:ミ:ソ = 4:5:6
- 単調　ラ:ド:ミ = 10:12:15
- C7　　= 20:25:30:36
- Cmaj7　　= 8:10:12:15
- C6　　= 12:15:18:20

もし宇宙人がいても

- 音波でコミュニケーションを取るなら
- ハモる現象は同じ
- 地球人に心地よい音楽は、宇宙人にとっても心地よいはず ？

Q & A

ご質問、ご意見ありましたら