

# 数学の社会的有用性に焦点をあてた暗号及び符号を題材とする教材開発

Development of Teaching Materials on Cryptography and Coding Methods  
Focusing on Social Usefulness of Mathematics at High Schools

成 田 雅 博\*      青 柳 広太郎\*\*  
NARITA Masahiro      AOYAGI Kotaro

**要約：**本研究では、数学の社会的有用性に焦点をあてた高等学校段階の教材開発を行った。多くの題材のなかから、高度情報社会のなかで、情報科学、コンピュータサイエンス、データサイエンスにおいて多用されている暗号及び符号に焦点をあてて教材を開発・評価した。

**キーワード：**高等学校，数学科，社会的有用性，暗号，符号

## 1. はじめに

数学科の授業、とりわけ高等学校段階においては、講義を主体とした教育方法や、目的意識が希薄で市販問題集や入試対策問題集のドリル学習による活動を主にした授業展開等、何のために数学を学習するのか、といった生徒の目的意識や意欲喚起をともなわない活動がみられる。本研究では、それに対し、数学学習の目的を達成することをめざし、数学の社会的有用性を実感する教材を開発した。

## 2. 数学の社会的有用性

本研究では、数学のよさのどの側面に焦点をあてて、教材を開発するかを検討するために、真田・大田（1995）の枠組みを援用することとした。

真田・大田（1995）では、鹿児島県内の公立中学校全数学科教師と、鹿児島県内から抽出された中学校9校の1～3学年の各2クラスの全生徒を対象に、数学のよさとして表1にあげた8つの観点をどの程度感じているかについて、アンケート調査（5件法による評定尺度法）を行い、数学科教師284名と生徒1986名から回答をえた。教師データ、生徒データの両方に対してそれぞれ因子分析を行った結果、以下のような分析結果が導き出された。

- ① 教師、生徒いずれの分析結果からも、数学のよさに関して、以下の3つの因子が抽出された（表1）。（真田・大田，1995，p. 12）
  - ・ 数学の考え方から数学のよさを感じる $\alpha$ 因子
  - ・ 数学の問題を解くことに数学のよさを感じる $\beta$ 因子
  - ・ 数学が役に立つ面に数学のよさを感じる $\gamma$ 因子
- ② 教師、特に男性教師は、主に $\alpha$ 因子及び $\beta$ 因子により数学のよさを感じるのに対し、生徒は、 $\beta$ 因子に加え $\gamma$ 因子からも数学のよさを感じている。（真田・大田，1995，p. 8）
- ③ 教師に関しては、それぞれの数学のよさを感じる因子の因子負荷量は年齢によって異なる。（真田・大田，1995，p. 4；pp. 8-9）

\* 教育実践創成講座（教職大学院）・附属教育実践総合センター

\*\* 大学院教育学研究科教職大学院の課程 教育実践創成専攻

表1 数学のよさの分類

| 因子名         | 数学のよさ    | 内容                |
|-------------|----------|-------------------|
| $\alpha$ 因子 | 論理性・確実性  | 論理の厳密さで結果が信頼できること |
|             | 優美性・審美性  | 得られた手法や結果が美しいこと   |
|             | 簡潔性・明確性  | 記号、式を用いて簡潔に表すこと   |
| $\beta$ 因子  | 娯楽性・ゲーム性 | 問題を解くこと自体が楽しいこと   |
|             | 充足性・優位性  | 難問等を解決できたときの満足感   |
| $\gamma$ 因子 | 有用性・実用性  | 実際に役立つこと          |
|             | 一般性・効率性  | 抽象化に起因する適応範囲の広いこと |
|             | 発展性・創造性  | 自由な思考により発展させられること |

また、数学のよさを感じ得る因子と教育方法、教材の構成に関して、以下のような考察もみられる。

「数学の問題を解くことに「よさ」を感じる $\beta$ 因子が、数学の考え方に「よさ」を感じる $\alpha$ 因子に先行していると考えられる。このことから、生徒に「よさ」を感じさせる場合に、授業の導入では〔充足性・優位性〕〔娯楽性・ゲーム性〕を感じさせるような場面を設定し、授業の展開では〔論理性・確実性〕〔簡潔性・明確性〕を感じさせるような場面を設定することが、教育方法の一つとして考えられる」(真田・大田, 1995, p. 12)

上の考察②から、本研究の目的である社会的有用性をはじめとする $\gamma$ 因子により数学のよさを実感する教材が、生徒により教育効果のあることが示唆され、その題材として本研究では、まず暗号を題材としてとりあげることにした。

教材の構成にあたっては、上記の考察をもとに、本研究においては授業の導入で $\beta$ 因子を、授業の展開では $\alpha$ 因子を主に生徒に感じさせるような場面を設定して授業を構成することとした。より具体的には、1時間目で行う暗号クイズ・各班で暗号をつくる活動が、娯楽性・ゲーム性を中心とする $\beta$ 因子に焦点をあてた活動となっており、その後の、合同式の性質が暗号のなかで用いられるようになった理由について学習する活動が、優美性・審美性を中心とする $\alpha$ 因子に焦点をあてた活動になる。このように、生徒が多様な数学のよさに触れるなかで、数学のよさを感じ得るよう教材を開発した。

本研究では数学のよさの $\gamma$ 因子の「有用性・実用性」に関して、数学がどのように役立って」いるのかについて、表2のように、さらに3つに分類して考察をすすめることとする。

表2 「役立つ」の分類 著者の一人(青柳)作成

|                                  |
|----------------------------------|
| 1. 私生活(自分自身の生活)で役立っていることを認識する。   |
| 2. 目に見える部分(日常生活)で役立っていることを認識する。  |
| 3. 目に見えない部分(社会生活)で役立っていることを認識する。 |

### 3. 暗号に関する教材開発

筆者の一人(青柳)は、2019年度、教職大学院の実習を行った連携協力校である中高一貫型高等学校1年生向けの暗号教材を開発した(青柳, 2020a; 青柳, 2020b)。その際、以下の先行研究を参考にした。

#### (1) 大澤(2001)の中学校第2学年対象とした授業

合計5時間の単元で、暗号の解説、暗号の作成、RSA暗号の理解について授業を行ったが、これは本稿第2節であげた数学のよさの「簡潔性・明確性」と「充足性・優位性」を生徒に認識させるための実践であると考えられる。この実践報告では、暗号の原理、特にRSA暗号の基礎にある、整数の合同式に関する理解や計算の技能修得が十分にできなかったためと思われる。

(2) 西村他 (2014) の、数学を専門としない社会人・大学生対象の公開講座

この講座では以下のようなテーマで3時間単位の講座を2回行っている。

1 回目は、1-1 暗号クイズ、1-2 暗号を作ろう、1-3 暗号の歴史Ⅰ、1-4 暗号と数学、2 回目は、2-1 単文字換字暗号(復習)、2-2 暗号の歴史Ⅱ、2-3 公開鍵暗号、2-4 RSA 暗号。この講座のねらいとしては数学のよさの「有用性・実用性」と「娯楽性・ゲーム性」があげられる。

(3) 岡本・伊禮 (2011) の高等学校第1学年を対象とした授業

この授業では、数学の有用性を生徒に実感させるために、①整数の性質の不思議さを感じ、その性質を理解すること、②整数の性質を用いて、課題を解決する「確認」の活動を行い、数学の有用性を実感することの2点を重視したRSA暗号の授業実践を行っている。授業実践後のアンケート結果の質問1『フェルマーの小定理について理解できましたか』に対する回答について次のように述べている。

「質問1において、「あまり理解できなかった・理解できなかった」と回答している生徒の数が多くなってしまった原因は、「 $\equiv$ 」と“mod”の理解が難しかったのであらうと考えられる。」(岡本・伊禮, 2011, p.93)

この考察から、授業の導入でフェルマーの小定理を扱い、RSA暗号について学習する前に“ $\equiv$ ”と“mod”を生徒に説明する時間が必要であると考え。そこで本研究では、合同式の学習を通して“ $\equiv$ ”と“mod”を生徒に理解させることを重視した授業を構想した。また、RSA暗号でなく、古典暗号系の1つであるシーザー暗号・アフィン暗号の構造を理解することを目的とすることで、暗号と整数の性質とのつながりを強く実感することができるよう授業を構想した。

以上から、授業内容を表3のように設定した。この授業では、①現在使用されている暗号の原点である古典暗号系を扱うことで有用性・実用性を感じ、②整数をある特定の自然数で割ったときの剰余に注目して整数の性質の不思議さを感じ、その性質を理解することで、優美性・審美性の感が期待できると考える。この授業のための提示教材を本稿巻末の資料1に示した。

表3 授業内容

|     |  |
|-----|--|
| 第1時 | 導入 : 暗号クイズ<br>展開1 : 暗号づくり (各班)<br>展開2 : 暗号の歴史と利用場面についての学習  |
| 第2時 | 導入 : 第1時に作成した他班の暗号解説<br>展開 : 合同式の定義・性質の学習  |
| 第3時 | 導入 : 第2時に学習した合同式の性質の証明<br>展開1 : 暗号以外の用途の学習 (教科書を中心とした問題演習),<br>展開2 : シーザー暗号の解説<br>展開3 : シーザー暗号とアフィン暗号を比較することを通して、数式が暗号のなかで用いられるようになった理由を知る |

## 4. 符号に関する教材開発

筆者の一人(成田)は、有限体を要素とする行列、ベクトルなどをつかった代数的符号を題材に、数学の有用性を学習者が実感することのできる教材を、高等学校数学科または情報科および大学の教養科目向けに開発した(NARITA, 2007)。

2010年度から2018年度にかけて行われた山梨大学テーマ別教養科目「数理の発想でみる自然・社会・人間」の教材として、本稿巻末の資料2が開発された。この教材は、主に大学初年度学生が履修する教養科目向けのものであるが、いわゆる文科系のコース、専攻等の学生も理解できるように開発しているため、少しの改変により高等学校でも使えると思われる。

### (1) 符号の基本的な仕組みと社会的有用性

この教材では、第2節の表2にあげた「3. 目に見えない部分（社会生活）」で役立つ側面をもつ、CD、DVD、USBメモリー等のデジタル記録媒体や、コンピュータ、スマートフォン、インターネットなどで必要不可欠な、情報ビットの誤りを検出したり訂正したりする符号（コード、coding）についての概説教材が最初に生徒が取り組む教材であり、その概要が付録2に提示されている。誤り検出符号の仕組みについては、兼宗（2020）の「コンピュータサイエンスアンプラグド」のなかの「カード交換の手品（エラー検出とエラー訂正）」で紹介されている。コンピュータサイエンスアンプラグドに関しては、兼宗（2007）を参照されたい。また、この教材の一部と教材評価に関しては、NARITA（2007）で報告されている。

## 5. まとめと今後の課題

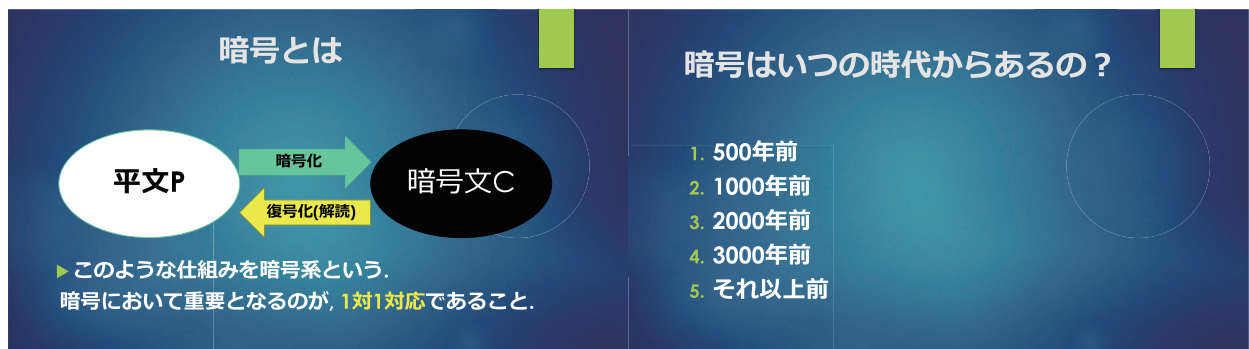
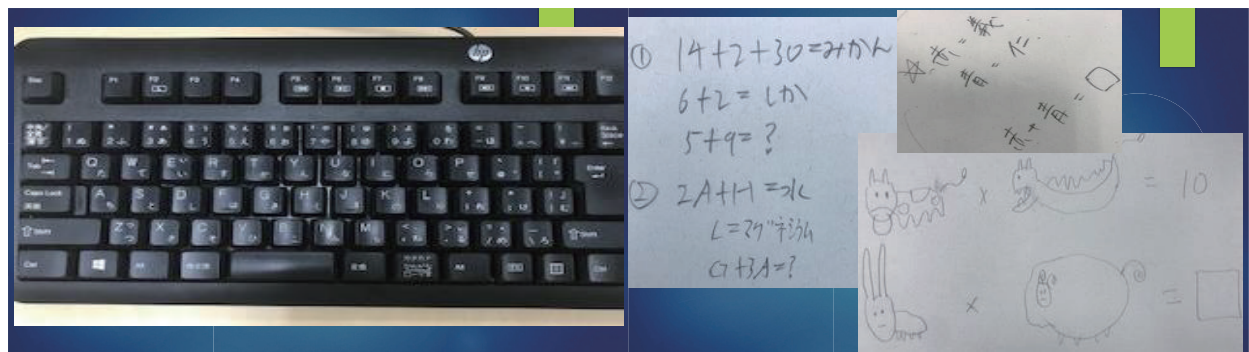
本研究においては、情報科学やコンピュータサイエンス等で多用されている暗号及び符号の教材について、これまでの教材を検討しながら、高等学校において利用できる教材のいくつかを提案した。今後は、関連文献との比較、評価や、教材の授業実践による評価によるブラッシュアップ、および社会的有用性を有する他の分野に関する教材、たとえば、金融数学、線形計画法をはじめとするOR（オペレーションズ・リサーチ）、グラフ理論、ゲーム理論等を題材とするものを開発することである。

### 参考文献

- 青柳広太郎（2020a）. 高校数学のよさを感じることのできる教科の開発 令和元年度 山梨大学教職大学院 教育実践研究報告書（8ページ）.
- 青柳広太郎（2020b）. 数学のよさに関する教材研究－有用性・審美性に焦点をあてて－ 日本数学教育学会第53回秋期研究大会発表集録，217-220.
- 市川伸一（2001）. 学ぶ意欲の心理学. PHP研究所.
- 兼宗進（2007）. コンピュータを使わない情報教育－アンプラグドコンピュータサイエンス イーテキスト研究所.
- 兼宗進（2020）. コンピュータサイエンスアンプラグド Retrieved by <https://csunplugged.jp/>（2020年11月26日）（Computer Science Education Research Group. CS Unplugged Retrieved by <https://www.csunplugged.org/en/topics/> の和訳）
- 川久保広臣（2013）. 数学における学ぶ意欲とその指導方法の研究－小・中・高での算数・数学教育を通して－ 高知県教育委員会.
- 松原元一編著（1987）. 考えさせる授業 算数・数学 東京書籍.
- NARITA, Masahiro（2007）. Curriculum for Teaching How Mathematics is Applied to Real World in Teacher Education Course at a Japanese College. In American Mathematical Society(Ed.), Enhancing University Mathematics: Proceedings of the First KAIST International Symposium on Teaching.－CBMS Issues in Mathematics Education(Vol. 14)－. 205-213. American Mathematical Society（Providence, RI, USA）.
- 西村保三・大久保裕介・佐分利豊・坪川武弘・福田浩之・松本智恵子・山下敏明（2014）. 暗号を題材にした数学の教材開発－H25 体験ふむふむ数学クラブ『暗号のすうり』の実践報告－福井大学教育実践研究，39，11-20.
- 岡本理生・伊禮三之（2011）. RSA暗号の教材化についての一考察 福井大学教育実践研究，35，87-95.
- 大澤弘典（2001）. 暗号の教材化についての一考察 日本数学教育学会誌，83(7)，10-17.
- 真田克彦・大田恭一郎（1995）. 『数学のよさ』についての認識調査－教師や生徒はどのように考え・感じているか－ 鹿児島大学教育学部研究紀要 教育科学編，46，1-18.



資料1 暗号の仕組み・簡単な暗号の紹介（導入教材・PowerPointスライド）



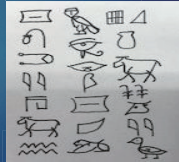
## 暗号の歴史

### ▶ 紀元前4~30世紀頃

#### ⇒ ヒエログリフ

古代エジプトの象形文字が**最古の暗号**と言われている。

⇒ 紀元前19世紀にロゼッタ・ストーンの研究が解読のきっかけに



## 暗号の歴史

### ▶ 紀元前6世紀頃

⇒ 古代ギリシャのスパルタで**スキュタレー暗号**が使われていた(3)。

送り手：棒に革紐を巻き付けて文字を書き、革紐を送る。

受け手：同じ太さの棒に巻き付けると解読できる。

転置式暗号方式



## 暗号の歴史

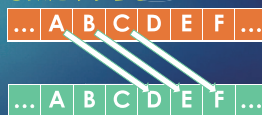
### ▶ 紀元前1世紀

⇒ ユリウス・カエサル(ジュリアス・シーザー)が用いた**シーザー暗号**と呼ばれる暗号方式(2, 4)。

暗号化  $f(P) = C \equiv P + b \pmod{26}$     復号化  $f^{-1}(C) = P \equiv C - b \pmod{26}$

⇒ 元の文章のアルファベットを**ある数だけずらし**て暗号化する暗号方式。

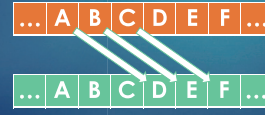
換字式暗号方式



暗号化  $f(P) = C \equiv P + 3 \pmod{26}$

例1. "FLY"を暗号化。

1. 数字に直す("FLY"⇒"5 11 24").
2. 法26のもとで3を足す("5 11 24"⇒"8 14 1").
3. 文字列に直す("8 14 1"⇒"IOB").

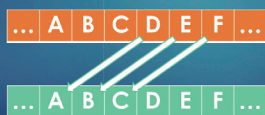


|    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|
| 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| A  | B  | C  | D  | E  | F  | G  | H  | I  | J  |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| K  | L  | M  | N  | O  | P  | Q  | R  | S  | T  |
| 20 | 21 | 22 | 23 | 24 | 25 |    |    |    |    |
| U  | V  | W  | X  | Y  | Z  |    |    |    |    |

復号化  $f^{-1}(C) = P \equiv C - 3 \pmod{26}$

例2. "NHB"を復号化

1. 数字に直す("NHB"⇒"13 7 1").
2. 法26のもとで3を引く("13 7 1"⇒"10 4 24").
3. 文字列に直す("10 4 24"⇒"KEY").



|    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|
| 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| A  | B  | C  | D  | E  | F  | G  | H  | I  | J  |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| K  | L  | M  | N  | O  | P  | Q  | R  | S  | T  |
| 20 | 21 | 22 | 23 | 24 | 25 |    |    |    |    |
| U  | V  | W  | X  | Y  | Z  |    |    |    |    |

## 暗号の歴史

暗号化  $f(P) = C \equiv aP + b \pmod{N}$

復号化  $f^{-1}(C) = P \equiv a'C + b' \pmod{N}$  ( $a' = a^{-1}, b' = -a^{-1}b$ )

アフィン暗号( $a = 1$ のとき、シーザー暗号)

どうして数式を使うようになったんだろう？

## 暗号を解読するためには

▶ 暗号を解読するためには**2種類の情報**が必要

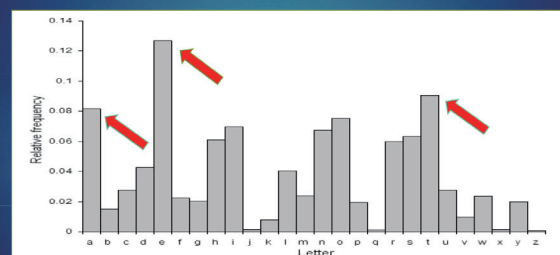
### 1. 暗号系の構造

例) アルファベット26文字、ひらがな50音順でずらすのか、置き換えるのか、など。

### 2. 暗号系の鍵

例) 「○文字ずらす」の○の部分(合同式の赤かった部分)。

## 1文字の場合(頻度解析)





### 暗号の歴史

15, 16世紀考えられた暗号

↓

ヴィジュネル暗号

### 暗号はどんなところで利用されていたんだろう？

### 暗号の利用場所

- ▶ 18世紀頃, **外交や軍事上**で暗号が用いられるようになった.
- ⇒ 安全性が求められるように.
- ▶ 19世紀頃に**無線通信**が実現したことで, 暗号が欠かせないものになった.
- ⇒ 機械式暗号装置(エニグマ等)の登場.

### 無線通信とは

### 暗号の利用場所

- ▶ これまでの暗号の利用場所は主に**軍事関係**だった.

コンピュータの出現

### 古典暗号系

### 公開鍵暗号

### 公開鍵暗号の仕組み

**P**

暗号化

$f: P \rightarrow C$

展開

計算が容易

←

計算が困難

?

**C**

復号化(解読)

$f^{-1}: C \rightarrow P$

因数分解

$pq = N$   
 $2 * 3 = 6$   
 $239 * 619 = 147941$

黄色の字の部分  
を公開

### RSA暗号

- ▶ 大きな素数を  $p, q (p \neq q)$  とし,  $n = pq$
- ▶  $GCD(\varphi(n), e) = 1$  となるような素数  $e (0 \leq e < \varphi(n))$
- ▶  $ed \equiv 1 \pmod{\varphi(n)}$  となる最小の整数を  $d (0 \leq d < \varphi(n))$
- ▶ 公開鍵  $K_E = (n, e)$ , 復号化鍵(秘密鍵)  $K_D = (d, p, q)$

$$C \equiv P^e \pmod{n} \text{(暗号化)}$$

$$P \equiv C^d \pmod{n} \text{(復号化)}$$

### RSA-129

11438162575788886766923577997614661201021829  
67212423625625618429357069352457338978305971  
235639587050589890751475992900268795435417

### サマーウォーズ

81438162575788886766923577992357799761466612  
01829672124236253625618429357069352457338978  
3059712356395870505898907514759929002687954  
35416

## 参考・引用文献

- ▶ N・コブリッツ著(1997)『数論アルゴリズムと楕円暗号理論入門』(櫻井幸一訳) シュプリンガー・フェアラーク東京株式会社 “

## 資料2 符号（コード）の仕組み

●コンピュータ内部では、すべての情報は0または1の数の列によって表現されている。ひとつひとつの0または1の桁をビット (bit) とよぶ。

※bitの語源は、binary digitである。binary＝2つの、2進法の。digit＝指、桁。

●符号化 (コーディング coding) とは、元になる情報（メッセージ）をあらかじめ決まった方法（ルール）にもとづいて、数に変換することである。変換された数のことを、符号語という。符号語全部を集めたもの（集合）を符号 (code) とよぶ。符号化された符号語をもとのメッセージにもどすことを復号化 (decoding) とよぶ。通常符号化する目的は、機械的に、特にコンピュータで情報を処理することであるので、符号化された数を2進表示（2進数表示）して0または1の数の列（ビット列）に変換する。

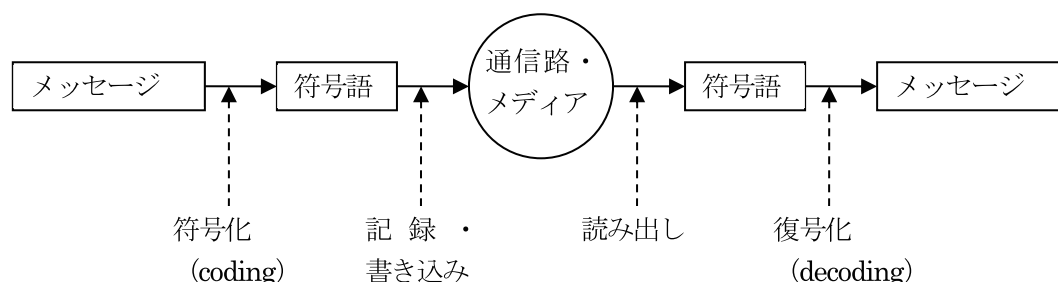


図2 符号化・復号化



●符号の例

- ・郵便番号 (zip code)
- ・JIS コード
- ・ASCII コード
- ・ISBN コード (書籍)
- ・バーコード
- ・QR コード (あるいは、2 次元コード)
- ・運転免許証番号 (偽造抑制のための応用)

●コンピュータで情報を扱うとき、CDなどの記録媒体のビット列を読み出すとき、一部のビットの読み出しが正しく行われなかったり、ディスクそのものに小さな傷があったり、ほこりチリ、回転のムラなどにより正しく読み込めなかったりすることがある。またネットワーク経由でデータを送受信するとき、ネットワークの経路上の雑音のため一部のビットに誤りが起こったりする。このようなことは、コンピュータに限らず電子的な情報をやりとりするあらゆる機会で見られる。たとえば、以下のような場合である。

- ・CD、CD-ROM、DVD、USB メモリー等へのデジタル情報の記録・読み出し
- ・衛星放送
- ・人工衛星や惑星探査機との通信
- ・クレジットカードやコンビニなどを使う際の決済情報の送受
- ・銀行、郵便局のATMにおいてキャッシュカード等を使った現金引き出し・決済等
- ・ネットショッピング・ネットバンキング

このような場合、1 ビットでも誤って読み書きされたり伝送されたりしてしまうと大きな問題が生じるので、誤りが起きたことを検出できる機能が必要であり、さらに可能ならば誤りが比較的に少ない場合には、誤りを訂正できる機能があることが必要である。

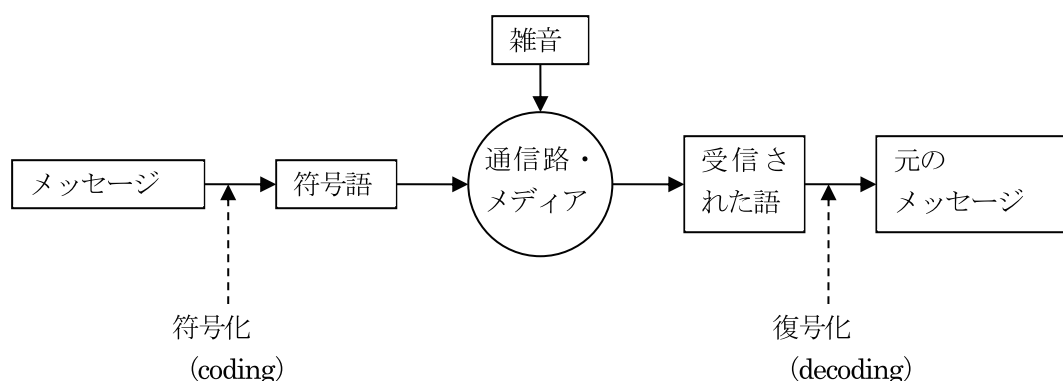


図3 雑音のある場合の符号化・復号化

●少数の誤りを検出する簡単なアイディア

- ・パリティチェック (parity check) ・チェックサム (check sum)

これは、広く使われている方法であり、符号の作成方法・誤り検出方法ともに単純（素朴・原始的）で計算も速くできる。

●実用化されているさまざまな符号（コード）

（１）バーコード

まず、以下の資料を読んでください。

朝日ソノラマ（1988）．バーコードのわかる本．朝日ソノラマ

裏辺金好&松戸合．第106回 これがバーコードの意味だ！（１）（雑学万歳）

[http://www.uraken.net/zatsugaku/zatsugaku\\_106.html](http://www.uraken.net/zatsugaku/zatsugaku_106.html) （2020年11月26日閲覧）

バーコード入門編／BARCODE HANDBOOK（株式会社テクニカル）

<http://www.technical.jp/barcode/> （2020年11月26日閲覧）

第4章 バーコードの体系－2：JAN(EAN)-8/13（2001年1月改正），5：主要なバーコードの種類と特徴（旧版 p.15）の「モジュラス10のウェイト3」が日本のコンビニや商店で多く使われているJANコードのチェックディジットのつけ方です。

バーコード情報サイト（日栄インテック）－バーコードとは？

<http://www.barcode.ne.jp/> （2020年11月26日閲覧）

（２）QRコード

まず、以下の資料を読んでください。

QRコードドットコム（株式会社デンソーウェーブ）

<http://www.qrcode.com/> （2020年11月26日閲覧）

QRコードをつくってみる

<http://www.swetake.com/qrcode/qr1.html> （2020年11月26日閲覧）

（３）書籍のISBNコード（International Standard Book Number・国際標準図書番号）

2006年までは10桁で構成されている（ISBN-10）。元のメッセージは9ケタの0～9の数字の列であり、10ケタ目が誤り検出用に使われる。

例1 4-408-05486-0（ブルーガイド編集部（2003）．ブルーガイド1泊2日・・・16 四国癒しの旅 実業之日本社）

例2 4-7628-2125-X（吉田 寿夫（1998）．本当にわかりやすいすごく大切なことが書いてあるごく初歩の統計の本．北大路書房）

例3 0-7645-5151-5（John Newman（1999）．Scuba Diving & Snorkeling for Dummies. Hungry Minds. New York）

1ケタ目：国，2～4ケタ目：出版社，5～9ケタ目：書籍名 を表す。

1～9ケタ目までの数を $x_1 \sim x_9$ とすると、誤り検出のための10ケタ目 $x_{10}$ は次のように計算する。

$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9$ を11で割った余りが10のとき $x_{10}$ を文字 X とする。

$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9$ を11で割った余りが10以外のときその余りをそのまま $x_{10}$ とする。

（４）運転免許証番号

第 **123456781230** 号 のように、12桁の番号の11桁目が誤り検出用に使われている（この場合の「誤り」は、具体的には偽造ということになる）。

# ●少数の誤りを訂正する簡単なアイディア

## ・重複送信

同じメッセージを3回続けて送る方法である。元のメッセージが1101だったら、110111011101を送信する。誤りの個数が1か所以下であれば、誤りを訂正できる。なぜなら、受信した符号語を4ケタごとに区切ってできる3つのブロックのうち2つは正しく送られてきたものであるからである。

●誤りの検出は元のメッセージのビット数より多くの「冗長な」ビットを付加して送る必要があり、誤りの訂正のためにはさらに多くのビットを付加する必要がある。しかし、ファイルのサイズを小さくして記録媒体を効率的に使ったり、通信を速くしたりするために、できるだけ少ない付加ビット数で誤りの検出・訂正をしたい。そのために、上記の方法より洗練した符号化の方法が開発されている。一方、機器の回路をできるだけ単純化してコストを下げるためにも、符号化及び復号化の手順（アルゴリズム）ができるだけ単純であるものを作りたい。そのような符号で実用化されているものの概要やアイディアを紹介しよう。実際には以下の説明より長いビット列を単位に符号化を行ったり、より洗練された手順を使ったりしているが、基本的には以下で紹介するアイディアと似ている。

## ●余りのみに着目した計算

以下では、パリティチェックのアイディアをすすめたものを行うが、和・差・積等の計算結果のある整数についての余りだけに着目してすすめていけばよいことになる。ここでは0か1の2つに1つであるので、演算結果は通常の計算の後2で割った余りとしておくことにする。

例：0+0=0, 0+1=1+0=1, 1+1=0, 0×0=0, 0×1=1×0=0, 1×1=1

これによって、 $-1=1$ ,  $1+1+1=1$

※数学の理論としては、ベクトルや行列の要素として有限体を考えていることになる。

あるいは、通常の数計算をしたあと、奇数→1、偶数→0、という置き換えをして考えてもよい。

## ●ハミング符号 (Hamming Code)

### ・(7, 4, 3)- ハミング符号

3次の行ベクトルのうち **0** 以外のものをすべてならべて書き出した行列を  $H$  とおく。

$$H = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\mathbf{x}H = \mathbf{0}$  となる（上の2で割った余りのみに着目した計算の意味で・・・mod2での合同） $\mathbf{x}$ のみを符号語とする。符号語は以下の16個になる。



$$\mathbf{x}_1 = (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)$$

$$\mathbf{x}_2 = (1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1)$$

$$\mathbf{x}_3 = (0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1)$$

$$\mathbf{x}_4 = (0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0)$$

$$\mathbf{x}_5 = (0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1)$$

$$\mathbf{x}_6 = (1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0)$$

$$\mathbf{x}_7 = (1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1)$$

$$\mathbf{x}_8 = (1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0)$$

$$\mathbf{x}_9 = (0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1)$$

$$\mathbf{x}_{10} = (0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0)$$

$$\mathbf{x}_{11} = (0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1)$$

$$\mathbf{x}_{12} = (0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0)$$

$$\mathbf{x}_{13} = (1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0)$$

$$\mathbf{x}_{14} = (1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1)$$

$$\mathbf{x}_{15} = (1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0)$$

$$\mathbf{x}_{16} = (1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1)$$

これらの符号語の任意の2つをとってくらべると、それぞれ異なるケタが3か所以上ある。このハミング符号を使った場合、伝送路で誤りが1ケタ以下しか生じない場合には、誤りの起こった箇所を特定することができ、送られてきた正しい符号語に自動的に訂正することができる。

この符号は、USBメモリーやRAID-2などのハードディスクの誤り制御などに用いられている。

●B.C.H. コード (Bose-Chaudhuri-Hocquenghem Code)

●リード・ソロモン符号 (Reed-Solomon Code)

この符号は、CD-ROMや音楽CD、QRコード等に採用されている。基本的なアイディアはハミング符号とも共通するが、もっと効率的な符号化、復号化ができる。音楽CD等では、通常前もって「先読み (バッファリング)」をしておき、この符号で復号化し、誤りが訂正できる場合は訂正し、訂正できない場合は正しく読み込めた前後のデータをもとに補間する等の処理をして、できるだけ音とびや雑音を避けている。また、リード・ソロモン符号による符号化を二重に施して、より多くの雑音に強くなるようにしている。代表的なリード・ソロモン符号は、RS (255, 223) であり、223ビットの情報ビットに対してパリティチェック用に32ビットが割り当てられており、16個の誤りまでなら正しく訂正できる。また、音楽CDなどでよくあるバースト誤り (連続したビットで起こる誤り) に強い符号である。