

数学による高大の連携と教材開発

渡辺 武志

[抄録] 高大の連携は学校で”出前授業”という形でいくつかおこなわれている。その内容は、大学の授業はどのようなものであるかを中心に、その研究内容やシラバス、授業の内容の講義など、生徒の知りたい内容を大学教官が伝えることが中心である。しかし単発の講義であるため、中等教育との接続が1回で完結する授業になるなど、次につながる授業ではないことが多く、改善が求められる。ここでは、高大の連携の1つのモデルとして、大学教官による授業について、その内容を活かした教材開発も行い、高大連携も視野に入れた新しい教科活動を紹介する。(2003年度新教科：自然と科学での授業内容)

[キーワード] 高大の連携 教科融合

1 高大連携への教材開発の流れ

新教科¹は週1単位半期の授業で、1つのクラスを3人の教員(理科・社会・数学)で3つのグループに分ける。そして必要に応じてT.Tで授業を行うなど、半期で1つの目標をもって授業を行う。今年度は

”DNAについてどこまで理解を深められるか”

を目標にその授業内容を考えた。しかし、数学教員としてはどのように手をつけるかわからずに理科・社会・数学の3人の教員による意見を出しあった。そこで、DNAをテーマにした話題で次のような知識の共有を図ることができた。

① DNAの塩基配列をもとにタンパク質が合成されるが、DNAを構成する塩基はA(アデニン)、G(グアニン)、T(チミン)、C(シトシン)の4種類であるが、タンパク質を構成するアミノ酸は20種類である。1個の塩基や2個の塩基の組み合わせではアミノ酸を指定するには数が足りない。よって、3個の塩基では $4 \times 4 \times 4 = 64$ 通りの組み合わせが可能であり、20種類のアミノ酸を区別することができる。(この考えは数学での暗号化、復号化の話に応用できる)

② 二進数、シーザー暗号(暗号化・復号化)について、その定義・歴史を社会と数学の2つの教科から光を当て、生徒の理解を深めることができる。

以上の観点で、教科横断的な授業配列を次のように行った。

- 第1回 (数学・理科グループのみ) DNAの抽出実験
- 第2回 (数学・社会グループのみ) モールス信号、暗号について(シーザー暗号)
- 第3回 大学教官(井原俊輔 名大・情報文化学部教授)による授業
- 第4回 DNAの各教科による考察
- 第5回 大学教官(久野 尚彦 名大・医学部助手)による授業

ただし、大学教官による授業が高校で授業がおこなわれているが、1回限りの授業ではなく、これらの授業の流れを構成する1つとして高大の連携を考えることに特に注意を払った。

この内容は、②の第2回、第3回の授業の内容である。

1.1 この内容の特徴

高大の連携が叫ばれている。従来は高等教育の内容を大学教官が授業するとき、中等教育での授業進度によっては、生徒がその内容の理解に差が生じる。これらのことを改善するため、

- (1) 事前に高校側での授業をする内容、そして大学教官の授業内容をあらかじめ確認する。
- (2) 高校側は大学教官が授業をする内容に予備知識が必要な場合、その授業の準備をする。

があげられる。大学教官の授業内容は50分(1時間)では短いため、あらかじめ内容の理解を深めるために、事前に生徒に宿題を出し、それをもとにした授業をあらかじめ中等教員が実施し、その宿題の内容も合わせて分析した。

¹新教科の目標、シラバスについては参考文献を参照

2 モールス信号・暗号について (シーザー暗号)

2.1 シーザー暗号について (授業の要旨)

情報の交換などで第三者にそれが知られないようにするためなど、対象となる情報を秘密にする技術や方法を暗号という。

最初に暗号を考えた人は紀元前1世紀のローマ時代にいたカエサル (シーザー) という人物である。当時ローマでは元老院支配が強く、当時の若い実力者3人 (ポンペイウス、カエサル、クラッスス) はこの支配を打破しようと、ポンペイウス、クラッススらと密約を結び、戦っていた。そしてガリア (フランス) 遠征時代にローマにいたポンペイウスとクラッススとの連絡のため、手紙の内容を見られないようにするために、ローマ文字を置き変えて書いたことがはじまりとされる。もとなる文章を平文といい、暗号化した文章を暗文という。

通信例は次のようになる。

(本人・原文から暗文)

・ABCDE から CDEFG

CDEFG を相手に送信すると、相手は暗文を平文に直す

(相手・暗文から平文)

・CDEFG から ABCDE

この場合、アルファベットの文字を2つずつずらしている。このような暗号をシーザー暗号という。

(授業ではプリントを配布し、シーザー暗号の解説や自分の名前を使ったアルファベットの変換などを行った。)

生徒のプリント

0717通信社 (7/25)

①紙→シーザー暗号

ローマ時代
ポンペイウス (ローマ軍団)
ガリア遠征 (ガリア軍)

②表

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

③ K A O R I T O Y A M A
N D R U L W R A P P D

自分の名前を暗号化しよう! (もとにもどせるかな?)

— K — A — — O — R —
— T — — — Y — —

④ 授業料 プリント
暗号を探る

1. シーザー暗号

シーザー暗号

OLV M P I A D
R O B P S L D G

⑤ 3-1
自1とく
も毛院先生
の暗号
暗号探検

⑥ 2. モールス暗号
ザシヨニル: モールス
1911~1912年

画家
1851年、印の中
1894年、ワシントン・ボルネオ7月の電信
ON-OFF

69年 東京 ~横浜

2.2 大学教官 (情報文化学部 井原俊輔 教授) による授業

以上の授業を踏まえ井原教官にお話したところ、50分の授業では時間が少ないため、次のような宿題を事前に生徒に出し、レポートを提出させた。

2.2.1 レポートの内容 (情報伝達をどう効率よく行うか)

考えてみましょう

モールス信号では短い電気信号・と長い電気信号——を使い、たとえばSは…Oは——で表します。緊急事態でSOSを打電するときは…——…を繰り返すこととなります。・を0、—を1で置き換えれば、モールス信号は各アルファベットの2進数列で表す信号といえます (0と1を並べた列のことを二進数列といいます)。たとえば、Sの符号語は000、Oの符号語は111となります。このような符号化を二進符号化といいます。

私たちが二進符号化を考えてみましょう。ただし、アルファベットはa, b, c, d, e, fの六個のみとします。各アルファベット毎に出現頻度は異なるものとします。このとき、次の条件 (1) (2) を満たす二進符号化を工夫してください。

(1) これらのアルファベットによる文章を符号化した2進数列を受信したとき、それから元の文章を正しく復元できること。

(2) これらのアルファベットによる文章を符号化した2進数列ができるだけ短くなること。

I. 次の場合にできるだけ良い2進符号を作ってください。

アルファベット a, b, c, d, e, f
出現頻度 $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \frac{1}{32}$
できましたか? それでは、次の文章を2進符号化してください。

bdaafabbcaaadbaacabeabacaaabbaca

I-1. 完成した符号列 (2進数列) から上の文章が正しく復元できますか?

I-2. 完成した符号列の長さはどれだけになりましたか?

II. Iと同様に次の場合にできるだけ良い2進符号を作ってください。

アルファベット a, b, c, d, e, f
出現頻度 $\frac{16}{30}, \frac{5}{30}, \frac{4}{30}, \frac{2}{30}, \frac{2}{30}, \frac{1}{30}$
できましたか? それでは、次の文章を2進符号化してください。

daafabecaaadbaacabeaacaabbaca

II-1. 完成した符号列 (2進数列) から上の文章が正しく復元できますか?

II-2. 完成した符号列の長さはどれだけになりましたか?

どのような考え方をしたら最適な符号を作成できるか、について6月28日 (金) にお話します。6月28日までに上の [I],[II] にチャレンジし、各自の解答を準備してきてください。(注意: この文章は無限個の文字列からとってきていて、出現頻度などは計算しやすいような値をとっている)

2.2.2 Iに関する生徒のレポートの解答、および分析

生徒には事前にアルファベットの例

”A,B,C,Dを0,1を使って暗号化するためにはA:00,B:01,C:10,D:11などのように0,1の組を考えて表さなければならぬ。”

についての知識は与えている。以下、主な生徒の解答について考える。

① アルファベットを2進数列に単純に符号化した解答

$a: 000, b: 001, c: 010, d: 011, e: 100, f: 101$

とすると、

bdaafabbcaaadbaacabeabacaaabbaca

は

001 011 000 000 101 000 001 001 010 000 000 000 011
001 000 000 010 000 001 100 000 001 000 010 000 000
000 001 001 000 010 000

と変換される。これについてはもとに戻すことができるが、文字の長さは $32 \times 3 = 96$ 文字となる。この問題では”できるだけ短い文字数で暗号化 (復号化) する”ことが目標であるからもう少し考察する必要がある。この解答が約3割あった。

② 出現頻度を考えた解答 (その1)

$a: 1, b: 01, c: 001, d: 0001, e: 00001, f: 000001$

とすると、

bdaafabbcaaadbaacabeabacaaabbaca

は

010001110000011010100111100010111001101

000011011001111010110011

と変換される。これらの解答は各アルファベットには出現頻度あり、

アルファベット	a, b, c, d, e, f
出現頻度	$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \frac{1}{32}$

であるから、出現頻度の高いものから短い文字列をあてると (この場合、文字の区切りを1とする。) アルファベットの列はかなり短くなる。

③ 出現頻度を考えた解答 (その2)

$a: 0, b: 10, c: 110, d: 1110, e: 11110, f: 111110$ とすると、

bdaafabbcaaadbaacabeabacaaabbaca

は

10111000111110010101100001110100011001011110
0100110000101001100

と変換される。出現頻度の高いものから短い文字列をあてると (この場合、文字の区切りを0とする。) アルファベットの列はかなり短くなる。今回の場合文字の長さは63文字。

②、③の解答が約5割いた。

④ その他の解答この文字列は有限個であるから、変換前の文字の共通性をみつけて変換した解答。

例1

$aa: 0000, ab: 0001, ac: 0010, ba: 0011, bb: 0100, bd: 0101, be: 0110, ca: 0111, db: 1000, fa: 1001$

例2

$d: 011, aa: 000, fa: 101, a: 100, be: 010, ca: 111, b: 001, bb: 110$

と考えると0,1の長さを64とした例。(この場合、アルファベットの出現頻度を考慮せず、有限個の出現頻度を考えた。) このような解答例は他にいくつかあげられる。

このような解答が2割いた

⑤ 変換できない例

$a: 0, b: 1, c: \frac{0}{0}, d: \frac{0}{1}, e: \frac{1}{0}, f: \frac{1}{1}$

もとに戻せない例が1割いた。

生徒のレポート

1年B組 番

考えてみましょう

[I] $a-1, b-10, c-100, d-1000, e-10000, f-100000$

10 1000 11 100000 1010100 111 1000 10 11 100 110 10000

1101 100 111 1010 1 1001

[I-1] *bdaafabbcaaadbaacabeabacaaabbaca*

[I-2] 63回 62回

[II] $a-1, b-10, c-100, d-1000, e-10000, f-100000$

1000 11 100000 110 10000 100 111 1000 10 11 100

110 100001 1100 11 10101 1001

[II-1] *daafabecaaadbaacabeabacaaabbaca*

[II-2] 62回 61回

2.2.3 井原教官の講義

情報伝達で大切なことは

信頼性および効率性

である。現在の通信はデジタル (0,1) 信号で送られる。”考えてみましょう”でもそのことが書かれているが、では、できるだけよい2進符号をどう作るかが課題となる。そこで、”考えてみよう”のIの問題についてかんがえる。

I. 次の文章を2進符号化してください。

bdaafabbcaaadbaacabeabacaabbaca

I-1. 完成した符号列 (2進数) から上の文章が正しく復元できますか?

I-2. 完成した符号列の長さはどれだけになりましたか? ただし、できるだけ良い2進符号を作ってください。但し、

アルファベット a, b, c, d, e, f

出現頻度 $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \frac{1}{32}$

です。その答えと必要な知識を表でまとめると、

①アルファベット	a	b	c	d	e	f	
②出現頻度	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{32}$	
③2進数列	000	001	010	011	100	101	96個
④2進数列 (最短)	0	10	110	1110	11110	11111	62個
⑤長さ	1	2	3	4	5	5	
⑥長さ	l_a	l_b	l_c	l_d	l_e	l_f	
出現頻度	P_a	P_b	P_c	P_d	P_e	P_f	

この場合、長さの期待値

$$L = \frac{16}{32} \times l_a + \frac{8}{32} \times l_b + \frac{4}{32} \times l_c + \frac{2}{32} \times l_d + \frac{1}{32} \times l_e + \frac{1}{32} \times l_f (= \frac{31}{16})$$

が最小になればよいから、それぞれの長さ l_i を調べればよい。

このとき、それぞれのアルファベットについて

○ある文章があつて、それを構成する1つの文字の出現頻度を p , とすると、必ず次のような長さ l がとれる。

$$2^{l-1} < \frac{1}{p} \leq 2^l \quad (-l \leq \log_2 p < 1-l) \dots (*)$$

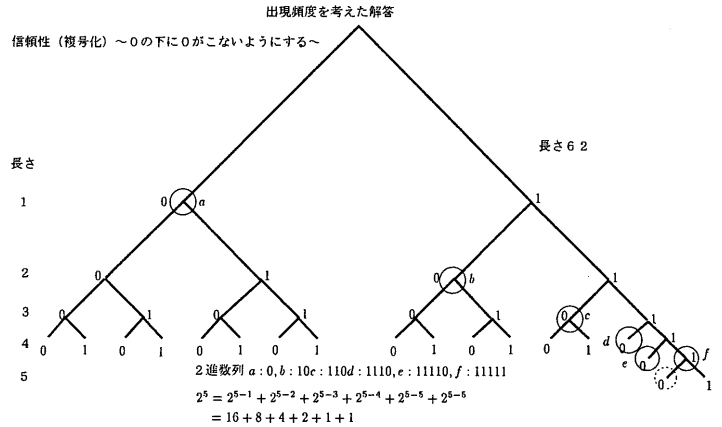
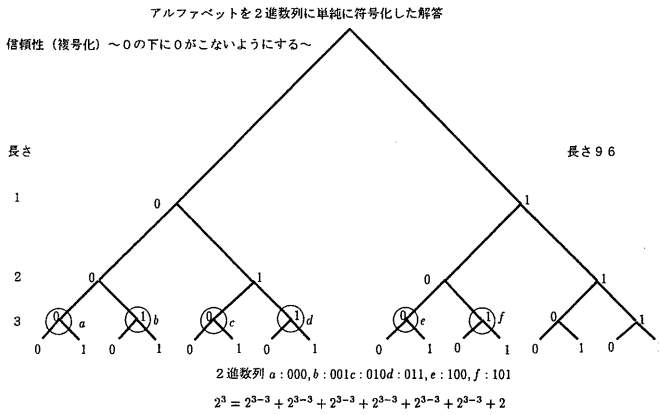
例) アルファベット d の出現頻度は $\frac{1}{16} = \frac{1}{2^4}$ より、

その長さ l_d を考えると、 $2^{l_d-1} < \frac{1}{p} \leq 2^{l_d}$ から

$$2^{l_d-1} < \frac{1}{\frac{1}{2^4}} \leq 2^{l_d} \text{. よって } l_d = 4.$$

つまり、アルファベット d の2進数列の長さは4となる。この長さを求めるには2進数列 0,1 より、次の樹形図を作成すると、うまくいく。

樹形図



出現頻度 (長さ) と樹形図との関係については、次の式がある

$$\sum_{i=1}^6 2^{-l_i} \leq 1 \iff 2^{l_{max}} = 2^{5-l_a} + 2^{5-l_b} + 2^{5-l_c} + 2^{5-l_d} + 2^{5-l_e} + 2^{5-l_f} + A$$

($l_{max} : l_a, l_b, l_c, l_d, l_e, l_f$ の中で最大の長さ) (特に各アルファベットの確率の和が1となるときの、閉じた樹形図 (剰余項 A が 0) を作成することができる)

○最小の長さの求め方は次のようにすると、うまく求められることがわかっている。

1. 各アルファベット①から出現頻度②を読み取る。
2. (*) 式に代入し、長さ l_i を求める。(求めた結果は⑤)
3. 最大の長さから、二進数についての樹形図を作成し、長さの短い (長い) 順から2進符号をふっていく。

3 今後の課題

高大の接続に関する内容は、勉学の必要性の一端を知ることができる面白い内容をたくさん含んでいる。しかし、大学入試の関係から、中等教育と高等教育の接続がうまくいかないことが現状である。これからは、この内容のように中等教育の知識を意識しつつ、高等教育の内容の一端を伝えて、生徒の目的意識も向上させることが確かな学力につながるのではないかと考える。

4 参考文献

新教科について

- ・新教科・暗号と DNA ~教材開発と高大の連携~ 渡辺武志 中野和之 西川陽子 2003年度名古屋大学教育学部附属中・高等学校紀要48集
- ・「高大の連携」を生かした「青年期のキャリア形成」平成13年度文部科学省研究開発学校研究開発報告書 他の新教科実践例について

・パイナップルをさまざまな角度から観察する

渡辺 武志 日本数学教育学会85回総会特別企画「公開授業」学習指導集・平成15年度

・暗号と DNA 渡辺 武志 第85回全国数学教育研究大会高等学校研究発表

暗号について

・理論と代数学 澤田 秀樹 海文堂,1997

井原教官の講義

・確率過程とエントロピー 井原 俊輔 岩波書店,1984