誤り訂正技術のしくみのデモンストレーション例 ―小学校の剰余計算の学習のみを前提とするリード・ソロモン符号の変形例―

中村博文 [1]

A Demonstration Example of Mechanism of Error Correction ―A Modification of Reed-Solomon Code Assuming Only Learning of Remainder Calculation at Elementary School―

Hirofumi NAKAMURA[1]

(平成 29 年 10 月 2 日受理)

あらまし　本論文は、記録や通信におけるデータの修復が、実際には計算でなされていることについて、小学校で習う剰余計算の学習のみを前提として、10～15 分でデモンストレーションする例の報告である。

具体的には、数枚のトランプの並びの中で 1 枚分の取り替えがあっても、取り替え前を知らない他者が計算で数を復元できる例を参加者皆で確認し、更に、なぜ復元できるかの理由を参加者皆が納得できることを目指したデモンストレーションである。

本校の毎年の科学イベントとなっている「おもしろ科学フェスティバル」において実施し、剰余計算を学習済みの小学生から大人までの殆どが内容を理解し納得できている。

記録や通信においてデータの一部が違ってしまう、即ち誤りが生じる、ということは、頻度は低いが日常的に起こっている。誤り訂正も現代の情報社会を裏方で支えている技術の一つであるが、例えば QR コードの一部をわざと隠したり汚したりして難なく読めるという実験をするというようなことでもなければ、データの修復をする誤り訂正技術の存在は意識することさえも難しい。本論文のデモンストレーションは、誤り訂正符号のひとつであるリード・ソロモン符号のアイデアを、トランプの数が 13 種類であり素数であることを利用した具体化と変形により、トランプ数枚の内の 1 枚分の誤り訂正の場合において小学 4 年生以上が納得できる内容になっている。決して単純ではないリード・ソロモン符号ではあるが、そのアイデアを、より知る人の多い、少ない数学的要素に落とし込む挑戦でもある。

キーワード　[出前授業，科学イベント，小学生，誤り訂正，リード・ソロモン符号]

1　序論

誤り訂正、暗号、データ圧縮、周波数帯の利用など、一定の制約のもとでの機能や性能を意識した情報の表現は、目に見える部分は極めてわずかではあるが現代社会を支える重要な技術の一部である。教育や紹介という観点からは、これらの技術に範囲を限っても、学課授業や出前授業、科学イベントなどにおいてどのようにしくみやアイデアの提示が可能かということは常に課題である。

本論文は、その中の、記録や通信におけるデータの修復が計算でなされていることについて、小学校

1 都城工業高等専門学校一般科目　　General Education Division, National Institute of Technology, Miyakonojo College

で習う剰余計算の学習のみを前提として、10～15 分でデモンストレーションする一例の報告である。

デモンストレーションの内容は、具体的には、数枚のトランプの並びの中で 1 枚分の取り替えがあっても、取り替え前を知らない他者が計算で数を復元できる例を参加者皆で確認し、更に、なぜ復元できるかの理由を参加者皆に説明するものである。

実際に、この後の２で述べるデモンストレーション内容を、小中学生等を主な対象とした本校の年 1 回の科学イベントである「おもしろ科学フェスティバル」（以下ではかぎ括弧を省く）において実施し、剰余計算を学習済みの小学生から大人までの殆どの参加者が内容を理解し納得できている。

このデモンストレーションの内容は、技術的には、QR コードや音楽用 CD、DVD、地上波ディジタル放送などで使われている誤り訂正符号であるリード・ソロモン符号[1)]と呼ばれる符号の原理を、トランプの数が 13 種類であり素数であることを利用した具体化と変形（３で述べる）により、1 シンボル（情報記号、デモンストレーションではトランプ 1 枚分）誤り訂正の場合において小学 4 年生以上が納得していける内容になっている。決して単純ではないリード・ソロモン符号ではあるが、そのアイデアを、より知る人の多い、少ない数学的要素に落とし込む挑戦でもある。

剰余計算だけは必須のため、このデモンストレーションの対象者としては、剰余計算が小学 3 年生の途中で習得する事柄であることから、その時期が境目（塾等で習っている場合は早まる）ということになるが、児童が慣れる期間も含めて、小学 4 年生以上であれば充分該当する。中高大学生や高専生、社会人も当然該当する。一方で、聞き逃すとしかけの肝心の面白いところが分からずに終わる点は年齢には無関係である。

また、このデモンストレーションの実施対象機会としては、趣旨や内容が合致し、準備や実施の時間が納まるなら、先に挙げた通り、学課授業の他、児童生徒の理数系への興味の一助や広く社会人も含めて紹介となるような出前授業や科学イベントなどが考えられる。

以下、まず２で本デモンストレーションの内容や進め方、３で機会や本デモンストレーション内容についてのきっかけになった事柄、４でパンフレット原稿について、５で本デモンストレーション例の符号化の別の場面での活用例、６ でおもしろ科学フェスティバルで実施した際の手ごたえや課題を述べる。

対象者に対しデモンストレーションを行う者（教職員でも学生や生徒でも）が知っておくべき最小限は次の２だけを見れば分かるように記載する。なお、デモンストレーションを行う者に誤り訂正や QR コード、リード･ソロモン符号の知識は必須ではない。もしこれらの知識量によって違いが出るとすれば、それはデモンストレーションの内容以外への質問あったときである。

小学生も対象にした科学イベントでのデモンストレーション内容へのみの関心で読まれることも想定し、誤り訂正の技術的な事柄や本校の授業との関連は、１と２では殆ど触れず、できるだけ３以降で述べる。

２　デモンストレーションの内容と進行

実施の実績はおもしろ科学フェスティバルにおいてであり、２．２に記した具体的な内容と進行例はその際のものである。読者がもし参考にされる際は、授業等場面の差異や、対象者の年齢や、参加希望者を募る方法等に応じて適宜取捨選択や改変をして下されば幸いである。読者が比較して他の場面に読み替えがし易いよう、ここでおもしろ科学フェスティバルについて若干触れておきたい。

おもしろ科学フェスティバルは年 1 回休日に 1 日で実施されている。数十ある出典ごとに必要なスペースに応じた場所が割り当てられ、必要な机・椅子や掲示スペース等も手配される。来場者は、配布されたパンフレット等を見ながら目的の出典を巡る場合もあるが、適当に巡りながら自発的にまたは出典の担当者に声をかけられて興味を持った出典に立ち寄る場合も多いようである。本論文のデモンストレーションは来場者に声をかけて参加して頂くことが圧倒的に多かった。

全体の開催時間帯は 10～16 時で、昼食で一時空けても 5 時間以上ある。その中で、このデモンストレーションは、開始時間を固定時間にはせず、空いている場合に随時受け付けたり随時声をかけて対応することにした。

平成 25､26 年度は同時にはほぼひと組ずつで参加者に応対した。平成 27 年度は A4 判のトランプと椅子十席程度を用意し一度に数組ずつの参加者に応対した。

２．１　進行について役割や準備など

以下では、イベントや授業でのデモンストレーションのその時点での対象者を参加者と呼ぶことにする。授業では大勢の場合もあり得る。参加者と書くが、おもしろ科学フェスティバルでは小学生や小学生を含む家族が多かった。

参加者に応対してデモンストレーションを行う者を実施者、その実施者の内訳を、進行役、追加役（のアシスタント）、訂正役（のアシスタント）と呼ぶことにする。

進行役と追加役は 1 人で兼ねてもよい。しかし、訂正役は、訂正ができることへの無用な疑念を参加者に抱かれないために、進行役や追加役とは別人がよい。よって、実施者はひと組 2～3 人である。筆者はおもしろ科学フェスティバルでは実施者ひと組のみで実施したが、もし複数組で対応すればそれだけ多くの参加者にランダム平行にデモンストレーションができる。教員が 1 人で行う授業の場合については、２．２(7)などで触れる。

本論文で、デモンストレーションに要する時間を 10～15 分と幅のある時間で記載するが、参加者への提示は 10～15 分の中のひとつの時間でも、幅のある時間でも、実施者間で意思疎通すれば任意である。なお、一日の中でも、内容の取捨選択の変更や、慣れによっても変化することは多い。

また、時間が余りない来場者にもできるだけ接して頂きたいということから、おもしろ科学フェスティバルでは、半分程度の時間も提示して応対した。

実施者は参加者の時間的都合に合わせるが、10～15 分程度で一通り終わるように進行する。おもしろ科学フェスティバルでは時間が 5､6 分程度しかない来場者にも、例として用意したものを用い、計算で訂正ができることだけは分かって頂けるよう心がけた。

デモンストレーションを実施する際の支援学生には後述の進行例を筆者が説明して流れを頭に入れて貰い、計算でデータの壊れが直せる一例については分かって頂くことが目的であることを伝え、基本部分は押さえて貰うがアドリブは構わないとして任せた。

支援学生の負荷を増さぬようリード・ソロモン符号やその他誤り訂正に関する事柄を予め教えることはこれまでは殆どしていない。デモンストレーションの内容以外への質問には、その場にいる者が知る範囲で対応することにした。筆者がいるときは学生が知らないことについて筆者が対応した。

トランプの 1 枚 1 枚は、エースからキングが 1 から 13 を表すという数にだけ注目し、マーク（ハート、クラブ等）は全く区別しない。デモンストレーションにおいて使用する数が重複することはよくあるため、トランプは 2 セット（エースからキングまでの 13 枚セットでいうと、8 セット程度）用意するのが望ましい。

次の２．２の進行内容例では、一部関連事項も記載する。準備内容にあたることの一部は再掲を避けるために、２．２の適所に記載する。

２．２　デモンストレーションの進行内容例

デモンストレーションの内容例を進行順に述べる。

おもしろ科学フェスティバルではパンフレットが作成され、このデモンストレーション用のページ（後ろの４で触れる）も 1 ページ分あるが、来場者は予め読んではいないという想定で進める。

実施者側の考えや、参加者等の時間的な都合に合わせて、実施者が適宜省く可能性の高い事柄には★印を付けている。

以下は進行内容の一例であるので、適宜、修正や改変、発展をするものとして読んで頂ければ幸いである。

(1)参加者に、QR コードなどで使われる、データが壊れた場合の修復の原理のデモンストレーションであることを告げる。

更に、もし小学生 3 年生以下が含まれていそうな場合は、後の種明かしのときに余りの計算を使うことを告げ、既学習かを尋ねる。未学習の場合には、種明かしのところは意味が分からないがそれで差し支えないかを確認する。もし諦めて立ち去る場合は 4 年生以上で機会があったらなどとフォローする。

(2)参加者に所要時間（10～15 分）を告げる。

科学イベントなどにおいては可能ならば、2 種類の時間（10～15 分及びこの半分程度）と、来場者の都合にも合わせられることを告げ、参加者に選んで頂く。

(3)予め印刷している QR コードを取り出す。【準備物：A4 判程度の用紙に QR コードの例を印刷しておく。筆者は本校 Web ページの URL を使用した。更に、一部をわざと汚したものも用意しておくとよいかも知れない。】

QR コードを示して、更に手または白や黒やその他のもので一部を隠して、それでもスマートフォン等で読み取れることを例示する（時間がないときは、口頭説明のみ）。URL の場合は、アクセスできることで確認できる。このとき、QR コードの四角の図形は QR コードの必須部分であるため、隠してはいけない。

ここの例のようにデータが一部違ってしまっても修復する技術のデモンストレーションであることを告げる。

この時点で実施者全員を紹介するかどうかは任意である。また、この時点で訂正役も紹介するかどうかも任意である。

訂正役は、後述するトランプでの符号化やトランプの取り替えの際には、その様子が見えない所で待機する。

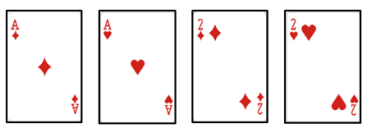
(4)進行役が、この後の進行内容として、簡単なマジック（手品他、表現は任意）と種明かしをすること、具体的には、参加者に 2 字の言葉を言っていただき、それをトランプの数字で表して、追加役のアシスタントが 2 枚追加して、その後、参加者にどれでも 1 枚何にでも代えて頂き、その後、別の訂正役のアシスタントが計算でどれが取り替えられていて元はどの数字であったかを突き止めること、更にその後で種明かしをすることを告げる。【準備として、進行内容を板書または掲示しておいてもよい。】

(5)時間があればできるだけ、意味のある 2 字の言葉を参加者に言って頂き、別表に基づいて、各文字について列と行をトランプ 1 枚ずつで、計トランプ 4 枚で表す。【掲示等で準備：50 音に濁音、拗音、促音も含め 10 列 10 行程度に配置し、列と行に数字を振った表（行も列も 1～13 の範囲を超えないこと）。この表で更に、列と行の数字の所に、対応する 2 進数を■と□で表したものを付記しておくと、参加者からの質問によっては回答が捗ることがある。4 ビット分なら 16 通りになるが、最大でも 13 通りしか載せないため、あくまでも参考用である。】

時間がない場合は、参加者に 4 枚並べて頂く。その時間もない場合は、進行役が適当な 4 枚を並べる。

ここで並べるのは、1 枚分訂正する場合なら、1～10 枚が可能であるが、ある程度の情報が盛り込め有用性が感じられやすいことと、計算量や説明の容易性から、筆者はこのように 4 枚で実施している。

この後文中に挿むトランプの例示は、言葉の例として「あき」を使った場合である（先述の 50 音表で、1 列目 1 行目と 2 列目 2 行目を想定）。



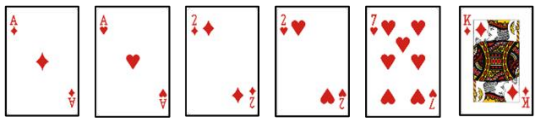
(6)符号化担当の追加役のアシスタントが右側に 2 枚追加する。

それは、全ての数の和が 13 で割り切れ、かつ、右から×1、×2、…、×6 とかけ算した値が 13 で割り切れるような 2 枚にする。以下は、13 で割った剰余を使う計算である。13 で割った剰余が等しいことを、単に「=」で表す。

例えば、追加した後の 6 枚を右から a, b, c, d, e, f、A=c+d+e+f、B=c×3+d×4+e×5+f×6 とすると、b=A-B、a=-A-b である。若しくは、C=c×2+d×3+e×4+f×5 とすると、b=A-B=-C=13+(-C)、a=-A-b= C-A でも算出できる。2 枚分の数の導出の仔細は追加役に任せる。

後々児童等参加者が自分にはできないと勘違いしないよう、コンピュータや電卓などは使わない方がよいと思われる。追加役がしている計算内容を参加者に見られるようにするかどうかは任意である。

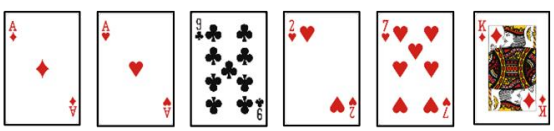
この間に、進行役から来場者に、種明かしは後ですることを念押しする。



(7) 参加者 1 名に、その時点のトランプ 6 枚の並びの 1 枚を、別に用意した 13 枚のどれかと取り替えて頂く。【準備物：エースからキングまでを直ぐ取れるような形で一式用意しておく。こうすることは、6 枚の中で場所の入れ替えをするのではないということが、明言しないでも分かって頂きやすい面もある。】

もし参加者に言葉を決めて頂いていた場合には尚更であるが、意図と異なる改変という雰囲気に繋がり易いよう、できるだけ言葉を決めた参加者とは異なる参加者に取り替えて頂く。

もし授業等で実施者が教員等 1 人のみの場合には、このときに、後ろ向きになるなど、取り替えているのを見ないでいる程度のことはした方がよい。



(8)★もし言葉をトランプで表していたら、変えた内容で元のデータの部分を言葉に直してみる。もし変な言葉になったら進行役がフォローする。

(9)進行役が、それまでの状況が見えない所で控えていた、訂正役のアシスタントを呼ぶ。

訂正役のアシスタントが、元に戻す計算をする。

例えば、S_1=a+b+c+d+e+f、S_2=a+ b×2+c×3+d×4+e×5+f×6 とするとき、S_1 と T をかけたのが S_2 になるような T が取り替えられたトランプの位置（右から 1 から数える）であるとして求められる。適宜、別途掲示等をしたかけ算表を用いる。この時点の位置 T のトランプに、その数から S_1 を減じた数のトランプ（13 で割った剰余が同じになるもの）を乗せる。

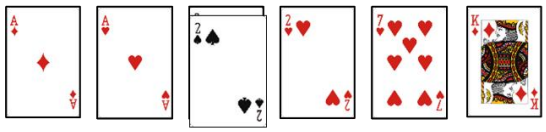
【掲示等準備：13 での剰余でのかけ算表を作成しておく。】

後々の不信感排除のために、参加者にこの時点の計算内容が見えるようにするかどうかは任意である。

ここでも、この間に進行役から来場者に、種明かしは後でることを言い添える。

訂正役のアシスタントは、トランプのカードを直す際には、更に上に置いて直す。この際に、どのトランプが入れ替わっていて、元の数字が何であったかを明言しながらの方がよい。

進行役が、元に戻ったことを、来場者と確認し共有する。



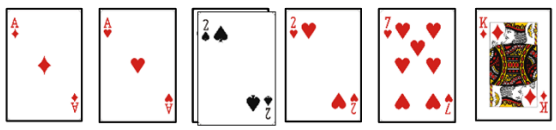
(10)進行役が、マジックはここまでで、このあと種明かしに入ること、分からないときはいつでも遠慮せずに直ぐに質問して頂きたいことを告げる。

(11) 進行役（または訂正役）が、以下のような種明かしをする。

まず、2 枚追加したときにどういう状態であったかを確認する。

具体的には、全ての数を足して、それが 13 の倍数であることを確認する。(エースからキングを 1〜13 として使うというのは、進行役が適宜口に出す。13 の倍数を載せた表を、適宜、必要に応じて参照する。)【掲示等準備：13 の倍数を載せた表を板書または印刷して用意しておく。】

また、右から×1、×2、…、×6 とかけ算した値を求め、それらを足して、それが 13 の倍数であることを確認する。【準備物：トランプ 6 枚分の幅で「×6…×2 ×1」と書いた紙を用意する。これをあてがうと説明が幾分捗る。】



2 つの計算のそれぞれで、13 で割った余りが 0 になるようにしていたことを確認する。

どこか取り替えたトランプが 1 だけ多い数字であった場合を一緒に考える。

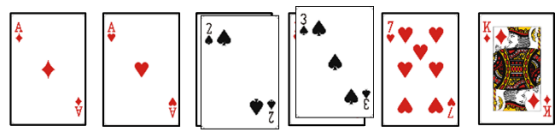
参加者が変えたのとは違う場所を進行役が決め、1 多い数のトランプを他から取り出して上に置く。(参加者が変えたのとは違う場所にするのは、より一般性を感じてもらうためであるがこだわらなくてもよい。)

1 多いトランプの場合に、全体の合計が 1 増えることを、一緒に確認する。(他のトランプは変化がないことと差分に注目すれば納得して頂き易い。必要なら適宜説明を補う。これまで、全てを足さないと納得されないことはなかった。)

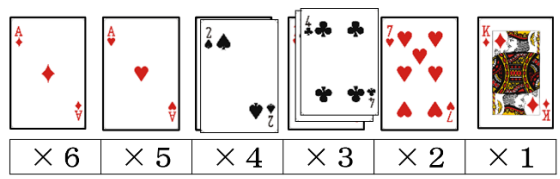
いくつ増えたかが、13 で割った余りで分かることを確認する。

ここだけでなく、計算内容の差分に注目した説明をすれば、手短かな説明で納得して頂き易い。

次に、もし 1 ヶ所が 1 増えたとき、右から×1、×2、...、×6 とかけ算した値がどれだけ変化するかを確認する。もし 3 番目なら 1 増えたから 3 増えるというようなことを確認する。



もし、例えば 2 増えたら、そのままの合計で 2 増えたことが分かり、2 と右から×1、×2、...、×6 のどれかかけた分だけ増える（6 増える）というようなことを確認する。

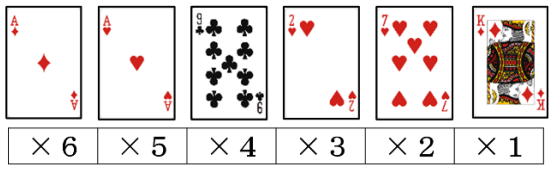


時間的に可能なら、または、参加者の理解のために必要と実施者が判断した場合は、更に 5 増えるとどうなるか（10 増える）のような例を追加する。

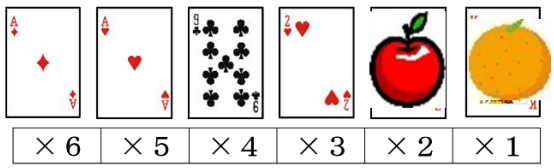
これらの際に、可能なら、質問を混ぜた形で参加者に確認する。

★かけ算表を指し、全ての場合がこれで分かることを告げる。

★(7)の結果に対する復元を一緒にやってみる。訂正前の合計を求め、13 で割った余り（13 の倍数の表を予め用意していれば、近い 13 の倍数を引いて求められる。）で、差分を知る。右から×1、×2、...、×6 をかけた値も用いて、表も適宜用いながら場所を知る。



★追加するトランプ 2 枚をどう選ぶかについて、（中学生以上では連立方程式と呼ぶものの求解を）果物で定式化から求解まで表した掲示物を用意して、2 枚の内容をどう決めたかに触れる（これはこれまで質問があった場合だけの使用が多かった）。【必ずしも必須ではないが、追加する 2 枚の数 a,b をそれぞれ異なる果物に置き換えて、具体例で果物が表す数の導出例を作成し掲示する。】



(12)★QR コードでは更に多く壊れても直せることや、もう少し難しい計算をしていることを告げる。
(13)★改めて質問がないか確認し、質問が出されたら適宜対応する。
(14)★データの修復を例にしたが、計算でいろいろな機能が果たせることや、実例や、有用性や、数学的要素を挿むなど、参加者の年齢等に応じて進行役が適宜まとめをする。

３　きっかけ

デモンストレーションの機会が生じたきっかけと、内容の着想のきっかけについて述べる。記述上必要なため、先にリード・ソロモン符号[1)]（ここから６までは、RS 符号と表記する）について触れておく。

３．１　RS 符号について

RS 符号の一般的な説明は他の文献に任せるが、この論文に必要な範囲で概略を述べる。デモンストレーション内容と RS 符号との共通点や差異に言及しない場合は読み飛ばされて差し支えない。

ｍビットで表せる 2^m通りの各情報を、拡大体 GF(2^m)の各元と同一視する。GF(2^m)の原始元をαと表す。情報のｍビットごとの区切りをブロックと呼ぶ。符号化や復号（誤り訂正を含む）は、送りたい情報のｋブロック×ｍビットごとに考える。以下ではこのｋブロック×ｍビット 1 式分について、1 シンボル誤りを前提として述べる。

ｋブロック分の情報が順に

a^0，a^1，･･･，a^{k-1}

であるとき、これをひとつの式で

$P(x)=a^0x^0+a^1x^1+\cdots,\ a^{k-1}x^{k-1}$

と表す。これは情報多項式などと呼ばれる。ここでは剰余の等価性だけでなく拡大体の元の等価性についても単に「=」で表す。

次に式

$G(x)=(x-\alpha^t)(x-\alpha^{t+1})$

を用いて、$x^2P(x)$を G(x)で割った剰余方程式を R(x)とする。ここでは最も簡単に t=0 とする。送信符号語として k+2 ブロックの

$F(x)=x^2P(x)-R(x)$

を用いる。G(x)は生成多項式と呼ばれる。F(x)は実際には、ビット表現にして記録または送信される。

F(x)を読み取りまたは受信した内容を、式として Y(x)と表し、更に

$S_1=Y(1)$、$S_2=Y(\alpha)$

とする。もし誤りがなければ、

$S_1=Y(1)=0$，$S_2=Y(\alpha)=0$

である。もし１シンボル誤りがあるとき、S_1が値のずれ具合を、$S_2\div S_1$をα^iと表したときの i が誤りブロックの位置（ゼロから数える）を表す（これらの証明は省略する）。S_1、S_2はシンドロームと呼ばれる。

もし１シンボル誤りではなく訂正できるブロック数を増やしたい場合には、その数 1 個ずつに対し G(x)に 2 個ずつ項を増やし、G(x)で割る前に P(x)にかける値を x^2倍ずつ増やす。このとき符号語のブロック数が 2 個ずつ増える。同時に、復号側で解くべき連立方程式や解の個数が 2 個ずつ増える。なお、符号語の訂正対象のブロック数は 2^m-1 が上界である。

RS 符号での拡大体の使用は、ビット列情報への適用の手段である。３．３との関連で先にここで述べておくと、もしデータの種類数（元の数）が 2^mの形式ではなく必ず素数であれば、選んだ素数の剰余で四則演算を行うことで足り、整数演算での理解が可能である。

３．２　デモンストレーション機会のきっかけ

教育機関等が在籍者以外、例えば近隣の児童生徒等に広く科学について紹介することや研究成果の一部を易しく伝える機会については、組織内の企画でや、また補助金等が外部から支援される場合も既に複数存在している。

そのような機会に参加者にいくつかでも種々の事

柄の効果を含め気付くきっかけを提示できたらとか、いくらかでも興味を持って頂けるような何らかのデモンストレーションをしたいという気持の他に、可能なら全くのブラックボックスのままではなく幾分でもしくみの一端も分かって頂ける所まで扱えないかという気持も生じる。

本校でも小学校等から依頼されて行う出前授業（や出前実験）は以前から学校として取り組んできており、著者も出前授業用でいくつか主に専門外のテーマしか用意できないできていたが、もしできるなら自分の専門分野の関連で参加者が面白いと思えることを実施できないかと悩んできたところである。

改めて検討した機会は、平成 25 年度から本校で毎年開催されているおもしろ科学フェスティバルの発足時である。なお、この催しへは誰でも参加できるが、主な対象は小中学生である（中学生や保護者を主対象としたオープンキャンパスが別途開催されていることもあるかもしれないが、実施してみると小学生が多かった)。学校等にも案内して来校した児童生徒等を対象に教職員等がテーマを決めてブースで実験等を行うが、できればオリジナルを目指し、筆者の知る限りで高校の教科書で多少なりとも扱われているのを見かけたアナログ／ディジタル変換、パリティ符号、ランレングス圧縮、RSA 暗号は避けたい気持ちがあった。

３．３　デモンストレーション内容のきっかけ

筆者が２に記載したようなデモンストレーション例に思いあたったのは、偶然を含め以下のような事柄が重なった結果である。それが、丁度本校で初めておもしろ科学フェスティバルを開催するために出展を募る時期にひとつに結実した。

(1) 筆者が専攻科の授業で、1 シンボル誤り訂正の RS 符号を、簡単な手計算を含む例題で扱っていたこと。

また、その際に、文献 2)を参考に、生成多項式に$(x-\alpha^0)=(x-1)$の項を含めて使っていて、(x-1)の項を含まない場合よりも簡単なシンドロームの計算に慣れていたこと。

そして、RS 符号の 1 シンボル誤り訂正では、シンドロームのひとつ（３．１での S_1）が誤った位置のシンボルの変化量を、もうひとつのシンドロームとの比のべき表現の指数（３．１での i）が誤りシンボルの位置を表すことを授業で確認してきたこと。

RS 符号で拡大体を使用する理由として、通常、情報の表現はビット列に基づいており、複数ビット即ち元の数が 2 のべき乗数での剰余で演算の解が一意になるためであることを確認してきたこと。

(2) QR コードは、現在の小学生が普通に使っているとまでは言えないが、近年よく見かけるものであること。また、一般の話題にはならないものの、実際に QR コードが RS 符号を使用していることと、QR コード（JIS X 0510：2004）の RS 符号では(x-1)の項が含まれていること。

(3) トランプはジョーカーを除くと札と数が 1 対 1 で対応していて、その数の種類が 13 で素数であること。エースからキングまでを 1～13 とすることも含め、小学生にもトランプはなじみがあること。そして、元が素数個の場合は、RS 符号において拡大体を用いず素数剰余の整数演算で代用ができる場合があること。

(4) RS 符号に基づくとき、整数演算で代用ができても剰余の計算が必要であるが、剰余の計算は小学 3 年生で学習しており、高専の学生には当然として、おもしろ科学フェスティバルの参加者の恐らく半数以上で理解可能と考えられたこと。

(5) 具体的に RS 符号似の計算で 1 シンボル誤りができることが、以下のように確認できること。

RS 符号について３．１のシンドロームの辺りまでの内容は再掲しない。以下は、それに続く部分として読んで頂きたい。

$S_1=Y(1)$は、シンボルの内容をそのまま足した値、$S_2=Y(\alpha)$は、シンボルの内容のそれぞれに順に 1、α、α^2、･･･をかけて、それを足した値である。

ここで、αの代わりに、例として 2 を用いてみる。ここから先の説明では、13 で割った剰余に注目した値である。

すると、2^0～2^{11}は、順に 1、2、4、8、3、6、12、11、9、5、10、7 である。

トランプのエースからキングが表す 1～13 の数をそのまま元として用いるものとする。13 は 0 と同じとする。

$S_1=Y(1)$は、RS 符号と同じく、トランプの数をそのまま足した値であり、置き換えたトランプの数がどれだけ増えたかを表す。

$S_2=Y(\alpha)$の算出で Y(x)の各係数にかける内容は、順に

1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7

である。

このままが RS 符号の直接的な整数表現(より詳しくは、更に 13 での剰余）であるが、次のように順序を入れ替えると、後述するように位置特定の計算がより簡単になる。なお、順序を入れ替えること自体は、RS 符号の機能に影響のない操作である。

つまり、トランプの枚数分だけ片側から順に

1，2，3，4，5，6，7，8，9，10，11，12
をかけたいということである。

途中でトランプを並べ替えることは煩雑である。そこで、元々片側から順に

1，2，3，4，5，6，7，8，9，10，11，12
がかけられるように並べていたものであると解釈しても差し支えがないため、実際そのようにする（このことを、小学生等来場者には特に断りを入れたり知らせることは省く）。

こうすると、S_2は、下位のシンボルから順に×1、×2、×3、×4、...とかけてそれを足した値になる。

もし、j 番目のシンボルが誤りのとき、$S_2 \div S_1 = Y(\alpha) \div Y(1) = j$ となり、この値が誤りシンボルの位置を与える。この計算式だけからはRS符号と異なるように見えるが、順番を変えたことでα^iの i ではなく、$\alpha^i = j$ の j が使えるようになったものである。j は1番目から数える。$S_2 \div S_1$の計算結果を誤りの位置の指標として用いていることは RS 符号と共通であるが、α^iの i の存在を告げないと変形した点はこの論文のデモンストレーションが RS 符号と異なる点である。

筆者にとっては、まず単純に総和と、×1、×2、×3、×4、…とかけて計算できるはずという直感が先で、以上のようにはその後で確認をしたという経緯であった。

(6)上記のように、トランプ1枚分(1シンボル分)の誤り訂正の場合は、計算の量が減らせていて、小学生とでもなんとか確認ができるくらいの量であること。

(7)多少の意外性若しくは驚きもありそうなこと。これが一番重要かもしれない。

筆者の専攻科での授業で RS 符号については、送信から受信の途中でビットが変わってしまう例を扱う際に、アドリブで、学生の誰かに板書内容を書き変えて貰って、それに対して誤り訂正を完了させていて、誤り訂正がうまくいくとまれに学生の小さい感動が伝わってくることがあったこと。

身近な存在であるバーコードに関して、情報の表現方法や誤り検出と、一定の条件下での誤り訂正について、専攻科の授業で触れているが、RS符号の方がやや意外性や達成感が大きいと思われたためこちらを選んだ。

２．２で述べた内容は、筆者の専攻科でのRS符号の授業を反映した点がある。それは、先述のように学生に誤りを作って貰うことと、具体例で誤り訂正がうまくいった後で種明かしを(専攻科では一般式で)するとそれも集中して聞いて貰える度合いが高いように感じていることである。一方、大きな違いは、専攻科では整数の剰余ではなく拡大体を用いていること、当然であるがα^iの i にあたる値で誤り位置を特定していること、符号化から誤り訂正までの全体に渡って理論的な一般式の学習をしながらその途中途中で具体例を挿み込みながら進めていることである。

トランプを2枚付加するというときに、上下左右とも考えられるが、最初にトランプで情報を表す際に特に断らないものの左から並べているため、この延長上にあるとの意味合いで筆者は右側に追加している。

また、×1、×2、…の演算順序を左端から考えるか、右端から考えるかについては、枚数が最初4枚と限定する必要はないため増減があっても付加する2枚のトランプの重みをその都度変えないようにと考えて、右端からにした。

おもしろ科学フェスティバルで訂正の原理の種明かしの際に、1 違いの誤り訂正を補助線的に先に説明すると分かって頂き易いのは、やって行くうちに分かったことである。また、訂正役がしっかり隠れて待機するのは学生が始めたことである。

４　配布資料について

先におもしろ科学フェスティバルでパンフレットが作成されると述べたが、近年は、出展ごとのページは、Web 上だけで、冊子体の配布パンフレットには収録されていない。

科学イベントの場合に参加者がパンフレット資料を予め読んでいることを前提にはできない（これは参加者に責任のあることではない)。学課授業や出前授業で事前に配布乃至はURLを連絡した場合でも、読んでいないことを想定する必要がある。この意味で、対象者に因らず**２．２**(4)は欠かせない。

しかし、パンフレット原稿の作成は少なからず時間を費やす。折角のことなので、少しでもより役立つようにと考え、当日に実施者が行う内容以外の事柄も「発展」として補足的に若干記している。

なお、保護者の中には参加前やデモンストレーションの最中にパンフレットを読まれて質問をされた方も若干名おられた。

本論文の最後に図1として次の実施に備えて準備中のパンフレット原稿案を示す（本校トップページ右上で「科学フェスティバル」などでサイト内検索すれば過去のパンフレット等へのリンクを含む Web ページがヒットする)。一般の方が恐らく既知ではない事柄を含めているのは、事後や帰宅後の閲覧に期

待しているためである。出展ごとのページが Web 掲載のみになっていることは先に述べたが、今後おもしろ科学フェスティバルで実施する際はブース内で配布したい考えである。

本校ではパンフレットにひらがなか読みがなの使用を申し合わせている。筆者は概ね小学 4 年生以降で習う漢字に読みがなを振っている（筆者は学年毎の未修得漢字をオレンジ工房提供の“小学校で習う漢字 チェックツール”http://orange-factory.com/tool/kanjicheck.html で確認している）。パンフレットは、印刷の際はモノクロになるものの、電子データではカラーも使用可能ということになっているため、トランプと Aha!の字に黒以外を使っている。

現象を見るものでなく、頭を働かせて体感して頂くものであることは、パンフレットでも強調している。

Aha! の気持ちを大事にしたいことの筆者にとってのきっかけはマーチン・ガードナーのいくつかの書籍である。そのことを多少表したいことと、テレビ番組の影響と勘違いされないようにとの気持ちから、最後に備考として記している。小学生も見るものではあるが、筆者が適訳を思いつかないことやガードナーの和訳書のタイトルでも使われているため英語表記をそのまま用いている。

小中学校への出前授業や本校低学年生への紹介であれば同じで済むと考えている。但し、本校低学年生に拡大体は用い難いが、提示資料を少し変えて、2^{i}の i（３．３(5)で述べた事柄）を誤り位置として用いた誤り訂正までは紹介可能と考えている。

５　拡大体不使用の RS 符号似の実用例について

RS 符号を拡大体を用いず整数のみの演算で具体化して、更に誤り位置を表すα^{i}の i に全く触れずにα^{i}の値を用いる誤り訂正の実用例については、寡聞にして他を知らないが、ひとつは次の実用例がある。

平成 25 年度の全国高等専門学校第 24 回プログラミングコンテストの競技部門課題（文字列をさいころの並びで符号化し必ず画像撮影して伝達する。受信側ではその画像データから文字列を再生する。競技時間内に文字を正確により多く伝達したら勝利。）のプログラム作品において、本校エントリーチームは競技者の並べ方のミスや画像認識プログラムの認識ミスがゼロではなかったことからこれらを充分カバーする程度の誤り訂正能力を持たせることにした。

学生が自発的に調べて本科授業で習わない数学に歯が立たないでいたが本論文と同様の符号化例を示したところ学生はさいころ 2 個分に使わない 1 パターンを加えて 37 進法にして整数演算（但し、37 で割った剰余に注目した演算）で済ますことをコンテスト作品の一部に取り入れて競技での確度を高めていた。ヒントが筆者由来であったため学生はコンテストのドキュメントで誤り訂正は全くアピールをしなかった。

ムダは 37 通り中の 1 通りで、データ量の 1%にも満たないということを確認した上での活用であった。勿論、算術符号を含むデータ圧縮は取り入れていた。

６　手ごたえと課題

６．１　おもしろ科学フェスティバルにおいて

本論文のデモンストレーションを実施した平成 25～27 年度のおもしろ科学フェスティバルをもとに述べる。

おもしろ科学フェスティバルとして来場者に毎回アンケートが実施されており、以下はその集計結果の一部を利用許可を頂いて述べるものである。

おもしろ科学フェスティバルへの来場者数は概数にすると 900 人、1500 人、2000 人（数値の並びはそれぞれ平成 25～27 年度、おもしろ科学フェスティバルとしては第 1～3 回、以下も列記は同様）で、アンケートへの回答者数は概数で 150 人、80 人、40 人であった。回答者数が最も多かった平成 25 年度を中心に述べる。

アンケートの中で「楽しかったイベント」という尋ね方で数十の出展の中から複数回答でマークする設問がある。

それによると、本論文のデモンストレーションの出展へのマークは、9 人であった。筆者のメモでは、参加者がひとりの場合も家族等の場合も 1 組として数えて、参加者は約 20 組であった。この比率からは健闘したのではないかと考えている。

保護者同伴でも小学生が 1、2 名の場合や、複数家族でも少人数の場合は、所々で確認しながら進めているため、殆どの参加者がよく理解したものと推測している。更に、発した言葉や表情から、計算で誤り訂正ができることについての小さな驚きを確信することも度々あった。

一方で、終了後に児童が立ち去る際に、難しいと言っているのが聞こえる場合が若干あった。しかし、それが、デモンストレーションの内容は理解してその上での発言なのか、デモンストレーションの内容で理解できないところがあったのかは、確認していない。

平成 27 年度には、A4 判のトランプを用い椅子を

十席程度用意して複数組が同時に参加できるようにした。参加者の人数や組数の記録を取っていなかったが､平成 25 年度の数倍の方が参加したという印象でいる。しかし、アンケートでマーク数の回答者比は増えていなかったため、何らかの反省点があると思われる。

筆者の推測になるが、大人数を対象としたため児童が納得できなくても質問がし辛かった可能性と、努めてマジックと明言した言い方をしたため過度の期待が生じた可能性が考えられる。

以下は、結論は出せていないが思案中の事柄である。

ほぼマンツーマンで応対する原則に戻るなら、実施者側で複数グループで対応することが考えられる。

複数組に同時に応対する場合には、子供への確認を密にすることや、そのため子供が前側に着席するような案内をすることが考えられる。

６．２　その他

追加する 2 枚のトランプの決め方については、今後の実施においては必ず少しでも触れるようにしてはと思案中である。

これまで、計算間違いという、言わばデモンストレーション上の大事故は幸いなかった。特に 2 枚追加する内容の間違いに気付かないで進めてしまうと全体を台無しにすることにもなりかねない。おもしろ科学フェスティバルでは筆者が参加者に応対しないときに一部で検算をしたが、万全を期すには可能なら恒常的に検算役を設けた方がよい。検算役は進行役による兼任も考えられる。現実的には、ミスの多少や、兼任の場合の負荷や、人数確保の難易度次第である。なお、特に誤り訂正の計算ミスを訂正役に知らせる方法には気をつけないと、参加者が疑念をもつことにつながる。

対象者が高校生程度以上なら、誤り位置に本来のリード・ソロモン符号と同様に 2^i の i（３．３(5)で述べた事柄）を使うことは大きな負担ではないと思われる。また、拡大体の紹介からはじめることも不可能ではないかも知れないが、これは 1 回あたりの実施時間との兼ね合いも含めて未検討である。

学課授業の内、本校の低学年の情報の授業では、使用する教科書やワーク教材によっては誤り検出や誤り訂正についてパリティ符号や垂直水平パリティ符号が載せられている（今後更に例は増えるかもしれない)。他の授業内容があることや本校の授業時間が平成 28 年度からひと区切り 95 分から 90 分に短縮されていることから、いつでも本報告の内容をデモンストレーションできる状態ではあるが、時間的な厳しさから今のところは教科書やワーク教材以上のことは見送っている状態である。どちらかというと、書籍などの商品コードなどでも使用されていて、バーコードなどと合わせて確認もできる、モデュラス 10・ウェイト 3 の方が先に触れるべき事柄と考えているところである。

誤り訂正符号のデモンストレーションとして高校生を対象とした中山ら[3)]の出前授業の取り組みを最近知った。30 分以上を想定し、スライド資料の他に、参加者がパソコンを使用する e-ラーニング教材や演習問題も用意されている点は特徴的である。もともと拡大体が不要な誤り訂正符号を題材にしているが、数式や行列表現を用いており、小中学生には無理な内容である。

７　結論

誤り訂正技術のひとつで QR コードなどに用いられているリード・ソロモン符号の原理のデモンストレーション例を報告した。

整数のみの演算になるよう具体化と変形をしているが、リード・ソロモン符号似の 1 記号誤り訂正を 10～15 分で小学 4 年生以上の殆どの参加者が内容を納得し理解できている。

本論文は電子情報通信学会情報理論研究会(「誤り訂正符号のワークショップ」と併催）における発表[4)]の内容をもとにまとめたものである。

謝辞

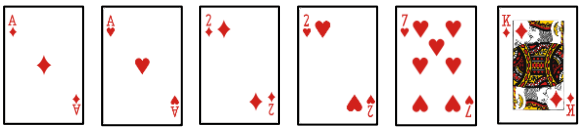
本校おもしろ科学フェスティバルにおいて支援頂いた方々、特に小学生等来場者に工夫しつつ終日一生懸命にデモンストレーションを行ったボランティアの支援学生各位に感謝します。

参考文献

1)I. S. Reed, and G. Solomon: Polynomial Codes Over Certain Finite Fields, J. Soc. Indust. Appl. Math., Vol.8, No.2, pp.300-304, Jun. 1960
2)三谷 政昭: RS 符号, やり直しのための工業数学, CQ 出版, pp.78-81, 2001（2001 年の版は絶版）
3)中山晃, 今井慈郎: 誤り訂正符号の学習を中心とした大学出前授業などで使用できる講義演習環境について, 電子情報通信学会技術研究報告, 教育工学研究会, Vol.116, No.517, ET2016-114, pp.117-122, March 2017
4)中村博文: リード・ソロモン符号似の 1 誤り訂正

の小学 4 年生以上への実演例, 電子情報通信学会
技術研究報告, 情報理論研究会, Vol.117, No.208,
IT2017-41, pp.15-20, Sept. 2017

データのこわれが直せるひみつ（実演）



所属　一般科目
担当者　中村　博文

【実施方法】あいていたら、いつでも始めます。データのかわりのトランプで、誰かが勝手に変えたのをあててみせます。**種明かし**のとき、算数の**あまりの計算**を使います。

【所要時間】１５分くらい（手品風の実演がない説明だけなら、半分くらいです）。

【はじめに】この実演は現象を見るものではありません。ＱＲコードなどのように**データのこわれが計算で直せる**のを、**頭で体験**します。現代社会を支えている「計算を使って役立つ働きを持たせるしかけ」の、ひとつの**ひらめき**を**体験**してみませんか。

aha!

【手品風のデータ修復のながれ】

データを決める	→	**だれかがデータを少しこわす**	→	**データを直す**
（ ① → ② ）	→	（ ③ → ④ ）	→	（ ⑤ → ⑥ ）

①伝えたい情報を決めていただき、**数で表します**（今日はトランプを使います）。
②アシスタントが計算して２枚足します（わけは、種明かしのときに分かります）。
③アドリブで、**トランプ１枚だけ**、自由に**変えていただきます**（どれかを別の数に）。
④トランプをそのまま**情報にもどしてみます**（ことばが変になっても笑わないで）。
⑤別のアシスタントが計算で直します。⑥情報にもどします（このあと種明かし）。

【データがこわれることについて】

データの**保存**や**伝達**は途中でデータの一部が変わってしまう（こわれる）ことがあります。ひとつのデータに注目してもめったに発見できませんが、身の回りにデータは多いので、実はあちこちで変わっています。対応として次のはどうでしょうか？
例:(1)信じて使う。(2)いつも送り主にきく。疑わしいなら(3)捨てる、(4)もっともらしく直す。

【こわれを直すことについて】

・直すために、前もって**データを追加**します。それは、**データを数におきかえて考えて**、いくつかの**計算**をゼロにするような値です。
・情報を白黒などで表していますが、主役は「数」です。今日はトランプで表します。
・ＱＲコードは、できあがりのデータの１割～３割がこわれても大丈夫です。今日は、トランプ何枚かのどの１枚を別の数に取り変えても、元どおりに直します。

発展・データの壊れを**誤り**、直すことを**誤り訂正**といいます。実は、誤りの数が許容範囲をこえると正しいデータを壊してしまうことと引きかえです。追加ﾃﾞｰﾀを増せば許容範囲も増えますが完璧はないです。上の例へのﾂｯｺﾐ例:迷惑では？⇒(1)～(4)、ﾃﾞｰﾀが正しいかそうでないか言い切れるの？⇒(2)～(4)。
・原理は通常見えませんが、沢山ある方式の内、今日はQRｺｰﾄﾞ、音楽用CD、DVD、地上波ﾃﾞｼﾞﾀﾙ放送などで使われる誤り訂正方式(ﾘｰﾄﾞ・ｿﾛﾓﾝ符号)の原理を体験します。今日は計算し易い例を用いますが、実際は白黒８つ(256 通り)毎に少し複雑な数(拡大体)が使われます。備考:自由研究にするときは提出先に確認を。QRｺｰﾄﾞは㈱ﾃﾞﾝｿｰｳｪｰﾌﾞの商標、無償特許で、ISO、JIS規格。aha!の語はﾏｰﾁﾝ・ｶﾞｰﾄﾞﾅｰの著書より。

図１　パンフレット原稿例