符号理論と数独

セキュリティ情報学　山口研究室　研究室紹介

研究内容

数独は世界中に愛好者がいるパズルだが、計算機による解答や問題作成などの様々な研究がある。本研究では数独が符号理論との対比で理解することができることを詳細に検討する。列や行などの数字を入れ替え異なる解への変更手法の提案を目標とし研究を行っている。

誤り訂正符号

誤り訂正符号とは、送信する符号に冗長(検査ビット)を持たせることによって通信路で発生する誤りを訂正する技術である。
消失通信路では入力に対して出力が正しい場合と消失する場合、誤った出力の場合、誤り訂正符号により正しい符号語に訂正をする。
図1,2に通信路と符号語の簡単な例を示す。

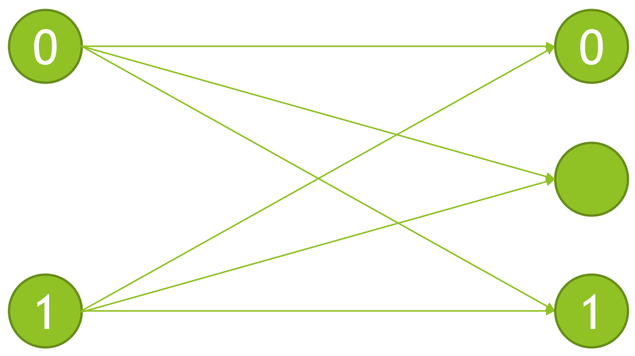

図1　2元消失通信路

図2は受信空間を表していて、各符号語の復号領域内の点を受信した場合正しく復号され、復号領域外の点を受信した場合訂正不可となる。また受信語が送信語と異なる復号領域内の点を受信した場合、誤訂正となる。
2つの符号語間の異なる文字の個数をハミング距離という。

数独と誤り訂正符号との比較

表1　数独と符号理論と誤り訂正符号の対応

パズルとしての数独	符号理論としてみた数独の理解	通常の誤り訂正符号
数独を解く	消失通信路における消失訂正	（消失でない）誤りの訂正
数独の解答	非線形符号の符号語	線形符号語
数独の問題	消失通信路を経て受信した受信語	誤りを含んだ受信語
ユニークな答えが求められない間違った問題	訂正不能な誤り検出	誤訂正、訂正不能な誤り検出
数独のすべての解答の集合	非線形符号（すべての符号語の集合）.	線形符号（すべての符号語の集合）
用いる記号 1-9の数字	体や環などの構造を持たない9種のシンボルにより定義される	GF(2)などのガロア体
ヒントの数 ヒント数の多い易しい問題	数独の解の世界を１つの非線形符号としてみた場合の最小距離は４	最小距離によって訂正能力が定められる

数独の制約条件はあらかじめマスに入れられた数字をヒントに1-9の数字を入れていき、行列、ブロックに1-9の数字が1回ずつ入る。1つの問題に対して唯一の答えを持つ。消失通信路における誤り訂正と数独を解く手順が類似していることに着目した。
通常、誤り訂正符号は線形符号であるが、符号理論としてみた数独の場合は非線形符号である。これらの対応を表1にまとめた。

数独の最小距離は4

誤り訂正符号として重要なパラメータである最小距離を検討した。その結果、数独の最小距離は4であるとわかった。

方法

数独における最小距離とは数独の異なる2つの解答(問題も異なる)を考え、この解にある81個の数値の間のハミング距離を調べる。

詳細

ある数値が4カ所異なる2つの解を想定する．1つの解が数独の解答として正しい条件を満たし，その数値のうちの4つをほかの数値に変えることができれば，これらの解のハミング距離は4となる．例としてあるブロック（αとする）内の同じ行に存在する2つの数字ａ,ｂがありそれと同じ列内で異なるブロック（βとする）中の同じ位置で、ｂ，aに入れ替わっておかれている様な解を想定する．
この４カ所の数字aとbを入れ替えたものは、
2つのブロックα，β内の条件，
4つの数値に関するすべての
行，列の条件に付いて
数独の性質を満たし，
その他の部分は元の解と
変わらず条件は満たされて
いるので，
新しい解を作成することができる．ゆえに数独の解の集合を誤り訂正符号としてみるとき、
その最小距離は４となる。

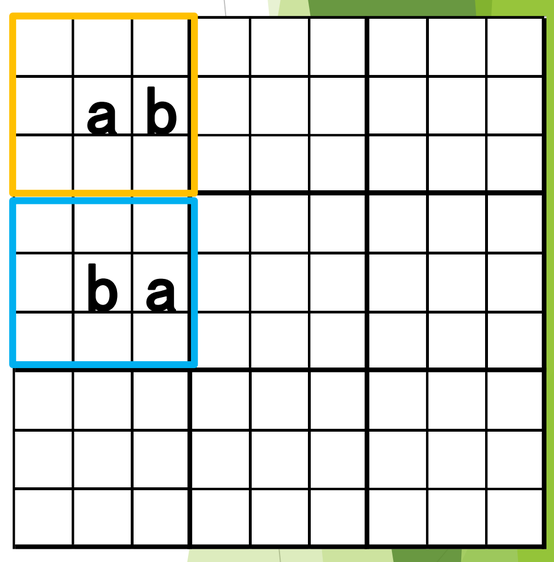

図2 別ブロック間の同位置に入れ替わって置かれた数値a,b

例として図3の数独の解答があり、赤の数字がa,bでそれらをひっくり返した場合も数独の解答として成り立つので、これらの２つの解の最小距離は4である。

7	2	3	8	6	5	9	4	1
1	5	9	7	4	8	6	8	3
8	6	4	1	3	9	2	5	7
5	9	8	3	7	4	1	6	2
2	7	1	9	8	6	5	3	4
4	3	6	5	2	1	7	9	8
3	4	5	6	1	7	8	2	9
6	1	2	4	9	8	3	7	5
9	8	7	2	5	3	4	1	6

図3　数独の解答

2	7	3	8	6	5	9	4	1
1	5	9	7	4	8	6	8	3
8	6	4	1	3	9	2	5	7
5	9	8	3	7	4	1	6	2
7	2	1	9	8	6	5	3	4
4	3	6	5	2	1	7	9	8
3	4	5	6	1	7	8	2	9
6	1	2	4	9	8	3	7	5
9	8	7	2	5	3	4	1	6

図4　図4の変形後

資料作成者：名波伸将