Cryptanalysis and Galois Theory

Shikata, Yoshihiro
Nagoya University

出版情報：MI lecture note series. 53, pp.1-8, 2013-12-26. 九州大学マス・フォア・インダストリ研究所
バージョン：
権利関係：

Keynote Lecture

Cryptanalysis and Galois Theory

Yoshihiro Shikata（Nagoya University）

From my experience during WW 2, I know Japanese took very light of information.
A part of which might be reflected in a certain characteristic of Japanese pure mathematics, not to mix well with practical mathematics, as informatics and/or statistics. For the future Japanese mathematics, it may be necessary to improve this situation, which could be the reason why we meet here together
First we take a look at coding and cipher:
As the coding system,we can count historical Caesar, Enigma method and modern RSA or algebraic curve method for future, Though the methods itself are different, every coding is based upon a permutation of alphabets. Therefore first attack on code may be done through comparison with linguistic rules as Magic decoding group, suggesting necessity of cooperation with linguistics.
On the other hand, Galois theory is a theory of the permutation group G, which asserts
1) To solve an algebraic equation of order k by algebraic method, the existence of a non trivial normal subgroup in G of order k is essential. Where we mean non trivial normal subgroup the normal subgroup except the normal subgroup of even permutation.
2) The permutation group G of order k (k>5) has no non trivial normal subgroup.
Thus we see, for example, that the normalizer of any subgroup of G essentially extends to G itself if k>5, which may give a theoretical background of successive replacement of alphabet in linguistic approach to attack code, .
Enigma system uses an embedding of alphabet into higher dimensional space and permutation of coordinate axis, plus rotations of the coordinate of the space, as a Rubik cube. Therefore it uses once a lift into a higher permutation group and then a splitting of the group into lower order permutation groups, plus the permutation of these small groups. Magic decoding group should have read the structure of thus obtained permutation. Here we may see fundamental symmetric polynomial help to find out the splitting, again a connection to Galois theory.
We can see a direct application of Galois theory to cipher in a sharing problem, proposed by Dr Aishiek. He proposed to decompose a word or picture printed in a sheet into two sheets, so that we read the original message if we lay these two sheets together. This

may be interpreted as a factorization problem of give message, and turns out to be a problem to find two roots (and another coefficient) of a quadratic equation for a given coefficient. Thus we may use direct Galois theory to measure the hardness of this cipher and the generalization possibility.

Another mathematical tool for coding and cipher may be topology for Galois simplex, which is Galois lattice admitting cell structure. Galois lattice is a lattice admitting hierarchy. If we introduce dimension and boundary to the component of the lattice so that they from a complex in accordance with the hierarchy, which we call Galois simplex, then they yield a homology of the lattice compatible with the hierarchy. we see that the homology is useful to measure the simplicity of the hierarchy.

The facts above are only several examples of the intersection of pure mathematics and the coding theory, other than well known prime number problem in RSA coding and algebraic curve approach for new coding theory. Thus we may expect a very fruitful results from further cooperation between pure mathematics and the coding theory.

My name is
Yoshihiro SHIKATA

四方義啓xysika@yahoo.co.jp

Born in 1936 in Kobe, JAPAN

Around 1936 many things happend

Military coup d'etat failed in Japan
Japan Germany anti communism treaty
Conflict between China

1936 was a turning point
Japan went direct to WW2

Japan US negotiation ended by Hull's note
Japan Russia peace treaty
Germans defeated at Moscow
Pearl harbor attack

The reality of the war made us realized
Japan makes light of information

Radio in Japanese fighter plane did not work well
Rader was considered a machine for cowards at first
Japanese pilots preferred Bomb than Rader

As for Cipher

Cipher decoding from Japenese side was not successful
American mathematicians breaked Japanese highest "purple cipher"

Around 1960

Graduated at Kyoto U
Master course
Specialized in topology and algebra
under Prof A.Komatsu

Around 1970

With Prof Klingenberg made
research on relation between
differential geometry and topology

Around 1975

Prof Thom of IHES
made aware of relation to
real world and mathematics

1980 was my turning point

Try to develop mathemaitics for real application
1980: Electronics and Mechanics → Gysi-simplex
1900:Medicine, Earthquake → EEG EMG
2000: Linguistics, Economy and Coding

Study of Coding and Pure math should be well related

Yoshi Shikata
四方義啓
xysika@yahoo.co.jp

Since Caesar, information is highly weighted not only in war field

Caesar cipher
Torch relay for exchange

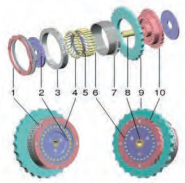
Cipher technique by machine are developed with war

Enigma coding and breaking
at the begining of WW2

Imbed alphabet into square matrix
Apply permutation to Raw and Column
↓
Enigma type coding

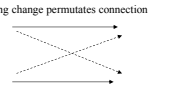
Real enigma system

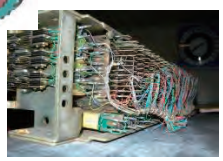
Combination of gear and wire
Gear rotates column and raw
Connecting wire switches connection



Gear rotation produce permutation

Wiring change permutates connection





Every coding at present depends on permutation of numbers

And embedding alphabet into
highler dimensional space of numbers

To realize permutation

Mathematical processing is useful
to generate the third number from given number
Add key number ⟶ Caesar cipher
Take a certain power ⟶ modern RSA
Algebraic curve and intersection for future coding
Enigma used decomposition and other besides arithmetic

Core of RSA coding is the following

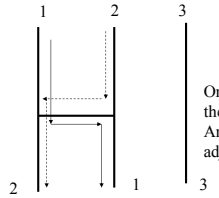
p^{th} power of x is x mod p
↓
$(p-1)^{th}$power of x=1 mod p
$(p-1)(q-1)^{th}$power of x=1 mod pq
$\{(p-1)(q-1)+1\}^{th}$power of x=x mod pq
↓
For any number KL=(p-1)(q-1)+1
KL^{th}power of x=x mod pq

Example in Mod 7 case

x	= 2,3,4,5,6
x square	= 4,2,2,4,1
x cube	= 1,6,1,6,6
x 4^{th}power	= 2,4,4,2,1
x 5^{th}power	= 4,5,2,3,6
x 6^{th}power	= 1,1,1,1,1

Representation of permutation by Amida kuji

One should take the woof line.till he meets the warp bar, then next woof line

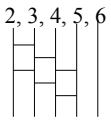


One can express all the permutations by Amida kuji adjusting the woof

Example of Amida kuji representation of 5th power in Mod 7

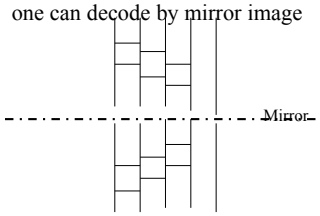
x = 2,3,4,5,6

$x^{5th power}$ = 4,5,2,3,6



Mirror image gives inverse or decoder

For given Amida kuji coding
one can decode by mirror image



Galois theory is a theory of Amida kuji

Problem: Does group of all Amida kuji decompose into smaller normal subgroups?

Answer: Over 5 woof lines it does not

↓

Even one seed grows to whole under "admissible operation"
indicates normal decoding is effective

Algebraic equation is equivalent to code the solution by its coefficient as fundamental symmetric polynomial

Galois thory

Possible to decode when the dgree is less than 5 by its normal subgroup

To transmit cipher 2 lines are used

One line to send the key of the cipher
Another line to send the cipher itself

Dr Avishiek's example
Sharing problem 1

He separates the 1 sheet image "IMBIC" into 2 sheets, each of which one not read but when the 2 is multiplied or doubled there appears letter "IMBIC"

This is interpreted as
the relation between solution and coefficient in quadratic eq

$\alpha\beta = c/a$

Avishiek send $\alpha\beta$ instead c/a

If the averaged use of lines are desirable

Then the fundamental polynomials should be used

↓

Up to 4th order it is possible

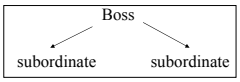
Over 5th order it looses "fairness"

For the sharing problem 2
we can use homology theory

Suppose there are
big bosses, bosses, subordinates

Topologist says

a boss and subordinates makes a family or 1 simplex if subordinates are connected to the boss by lines

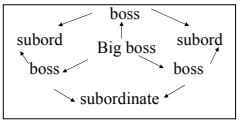


1-simplex

Suppose there are
big bosses, bosses, subordinates

Topologist says

a big, boss and subordinates makes a family or 2 simplex if they are well connected to the big boss



2-simplex

Those 1,2simplices have face

Every k-simplex are requested to have k-1 boundary to meet another family

The boundary of boundary is required to be zero

The relation boss and face can be replaced by priority of order

If here is no hole or
"homology is zero"
then the complex is well ordered