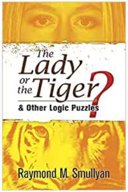
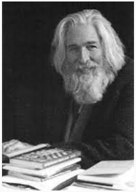
The Monte Carlo Lock

Fall 2022 - R. L. Herman





Introduction

The Monte Carlo Lock Puzzle is from Smullyan's *The Lady of the Tiger & Other Logic Puzzles.*

- Inspector Craig is called to a case.
- The safe combination (on one card) was lost.
- Martin Farkus, a mathematician, left clues about code.
- The safe has to be opened by June 1, or it is blown.
- The code has capital letters of any length and may be repeated.
- Entering a code will

    Open the lock.
    Jam the lock, or
    It does nothing (neutral).

Goal Use Farkus' clues to open the lock.

Farkas' Clues

Denoting xy as the concatenation of the codes x and y, then for any letter combinations x and y, there are "special relations" satisfying the properties below.

Property Q: For any combination x, the combination QxQ is specially related to x.

Property L: If x is specially related to y, then Lx is specially related to Qy.

Property V (the reversal property: If x is specially related to y, then Vx is specially related to the reverse of y.

Property R (the repetition property: If x is specially related to y, then Rx is specially related to yy.

Property Sp: If x is specially related to y, then if x jams the lock, y is neutral, and if x is neutral, then y jams the lock.

Symbolic Summary of Clues

We write $y \to x$ to mean "x is specially related to y." Then,

- The code contains the letters L, Q, R, V.
- Denote xy as the concatenation of the codes x and y.
- Use $\overleftarrow{y}$ for the reverse order of the code y.

For codes x and y, the following are true:

- Q: $x \to QxQ$.
- L: If $y \to x$, then $Qy \to Lx$,
- V: If $y \to x$, then $\overleftarrow{y} \to Vx$,
- R: If $y \to x$, then $yy \to Rx$.

Craig surmised that a code x opens the safe if and only if $x \to x$. [1]

[1] From Property Sp, if $x \to x$, then x both jams the lock and is neutral. This contradiction implies that x must open the lock.

A Curious Number Machine

Before attempting to solve the Monte Carlo Lock Problem, Inspector Craig visits Norman McCulloch, who has developed a number machine.

Chapter 9: Started with two rules.

Chapter 10: Added two new rules and learned about Craig's Law.

Chapter 11: Fergusson's Laws.

Chapter 13: The Key to the Lock!

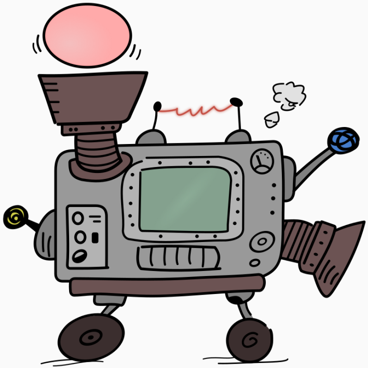


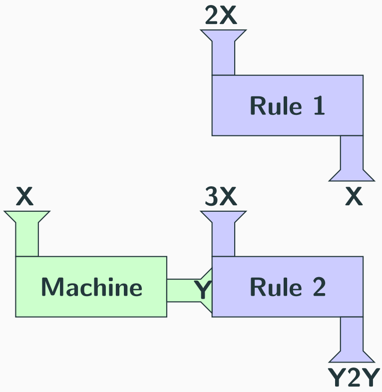
Figure 1: Number in, number out.

McCulloch's First Number Machine

- Only acceptable numbers.
- Deterministic rules.
- N - positive whole number.
- No 0's.
- NM - Concatenation.
- Rules: If $X \to Y$,

  1: $2X \to X$. (Erase 2.)

  2: $3X \to Y2Y$. (Associate of Y)



32586 ⟶ [$\mathbf{3}2586 \to Y2Y$; $\mathbf{2}586 \to 586 = Y$] ⟶ 5862586

Leads to Puzzles

$$\mathbf{32}586 \longrightarrow \boxed{\begin{array}{c}\mathbf{3}2586 \to Y2Y \\ \mathbf{2}586 \to 586\end{array}} \longrightarrow 5862586$$

Only acceptable numbers begin with 2 or 3. But not all 3's, 32, 332, etc.

$2X \to X$;

$32X \to$ Associate of X, $X2X$;

$332X \to$ Double Associate of X, $X2X2X2X$;

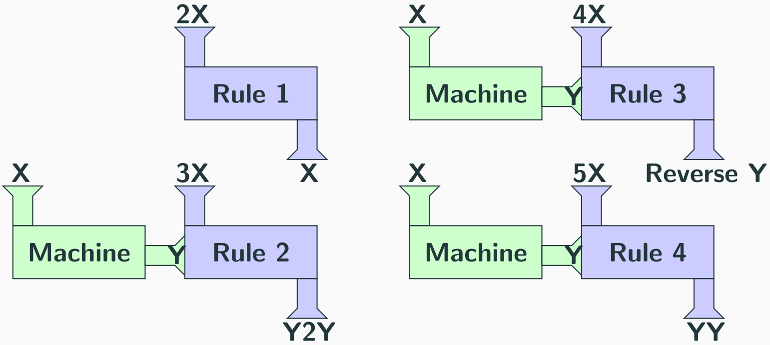
$3332X \to$ Triple Associate of X, $X2X2X2X2X2X2X2X$; etc.

Problems

1. $N \to N$?
2. $N \to N2N$?
5. $N \to 7N$?
6. $3N \to N2N$?
7. $N \to 3N23N$?
8. $Y \to AY$? McCulloch's Law.

Ch. 10 McCulloch's Second Machine - 4 Rules

Rules 2-4: $X \to Y$.



1: $2X \to X$. (Erase 2.)

2: $3X \to Y2Y$. (Associate of Y)

3: $4X \to \overleftarrow{Y}$. (Reverse Y)

4: $5X \to YY$. (Repeat Y)

Using Rules 3 and 4

1: $2X \to X$. (Erase 2.)

2: $3X \to Y2Y$. (Associate of Y)

3: $4X \to \overleftarrow{Y}$. (Reverse Y)

4: $5X \to YY$. (Repeat Y)

Apply Rule 3: Pick $Y = 7695$. Find X such that $X \to Y$, $X = 27695$.
Input $4X$ into the machine:

427695 ⟶ [**4**27695 → Reverse 7695; **2**7695 → 7695] ⟶ 5967

Apply Rule 4: $527695 \to YY = 76957695$.

Problems

1. $N \to N$? (Before, $N = 323$.)
2. Find nonsymmetric number.
3. $N \to$ associate of reverse?
4. $N \to NN$.
5. $N \to \overleftarrow{NN}$
7. For any X, $52X \to XX$.
   Find X, so that $5X \to XX$.

Inspector Craig's Number Operations

Craig realized that many problems could be solved using one principle.

"There must be a number that produces the repeat of the of the reverse of its own associate, and a number that produces the associate of the repeat own reverse, and a number that — " - pg. 127.

Craig introduces *operations* on $X : F(X)$ and *operation numbers,* M, such that $MX \to F(X)$.

Examples

a. 4 determines reversal.
b. 5 determines repetition.
c. 3 determines association.
d. 35 determines associate of repeat.
e. 45 determines reverse of repeat.
f. 54 determines repeat of reverse.
   Last two give same result.
g. What does 44 represent?

Inspector Craig's Observations

Let operation number M determine $M(X)$. This is not MX : $3(5) = 525$ not 35.

Many previous problems of form:

> Find a number X that produces its own repeat, $X \to 5(X)$.
>
> Find a number X that produces its own associate, $X \to 3(X)$.
>
> Find a number X that produces its own reverse, $X \to 4(X)$.

Given operation number M, find X such that $X \to M(X)$.

Example: $X \to 543(X)$, repeat of reverse of the associate of X.

Example: $X \to 354(X)$, associate of repeat of the reverse of X.

Example: $X \to 5433(X)$, repeat of reverse of the double associate of X.

Last Fact: For any operation number M and any numbers Y and Z, if $Y \to Z$, then $MY \to M(Z)$. [If $35 \to 525$, $535 \to 5(525) = 525525$.]

Craig's Laws

Law 1 For any operation number M, there must be some number X that produces $M(X)$.

Law 2 Given any operation number M and any number A, there must be some number X that produces $M(AX)$.

Find $Y \rightarrow AMY$. Then, $MY \rightarrow M(AMY)$. For $X = MY$, $X \rightarrow M(AX)$.

Consider $Y = 32AM3$. Noting that $32AM3 \rightarrow AM32AM3 = AMY$, then, $X = MY = M32AM3 \rightarrow M(AX)$

Example: 21 $X \rightarrow 7X7X$, repeat of $7X$. Let $A = 7$ and $M = 5$. So, $X = 532753$.

Example: 22 $X \rightarrow$ reverse of $9X$. Let $A = 9$ and $M = 4$. $X = 432943$.

Example: 23 $X \rightarrow$ assoc. of $89X$. Let $A = 89$, $M = 3$. $X = 3328933$.

Example # 23: Verification of the result

Find X : $X \to$ associate of $89X$. Answer: $X = 3328933$.

3328933 ⟶

3328933 $\to Z2Z$, associate of Z.
328933 $\to Y2Y = Z$, associate of Y.
28933 $\to 8933 = Y$, erase 2.

⟶ $Z2Z$

Therefore, we have

$$\begin{aligned} 3328933 \to Z2Z &= Y2Y2Y2Y \\ &= 8933289332893328933. \end{aligned} \tag{1}$$

What is the associate of $89X$?

$$89X289X = 8933289332893328933.$$

Note: $Y2Y2Y2Y$ is the double associate of Y.

Fergusson's Laws

Malcolm Fergusson, logician and student of Gottlob Frege (1848-1925).

Introduced by Craig, he found new properties of the machines.

Prob. 1 The exists X, Y such that $X \to \overleftarrow{Y}$ and $Y \to XX$.

Example: $X = 4325243$, $Y = 524325243$.[2]

Prob. 2 Find X, Y such that $X \to YY$ and $Y \to \overleftarrow{X2X}$.

Fergusson's First Law:

Given M, N there exists X, Y such that $X \to M(Y)$, $Y \to N(X)$.

To prove, one considers using Machine 1 (Rules 1,2).

Find $X \neq Y$ for numbers A, B, such that

2. $X \to Y$, $Y \to X$.
3. $X \to Y$, $Y \to AX$.
5. $X \to AY$, $Y \to BX$.
6. Use Craig's 2nd law to prove Fergusson's.

[2] Like pulling rabbits out of a hat!

More Fergusson Laws

Double analogue of Craig's Second Law: Given two operations M and N and two numbers A and B, do there exist X, Y such that $X \to M(AY)$ and $Y \to N(BX)$.

Example 7 $X \to 7X7X$, $Y \to \overleftarrow{89X}$.

Given operation M, number B, find X, Y such that $X \to M(Y)$ and $Y \to BX$.

Example 8 $X \to Y2Y$, $Y \to 78X$.

Triplicates and Beyond

There are numbers X, Y, Z such that $X \to \overleftarrow{Y}$, $Y \to ZZ$, $Z \to X2X$.

$X = \mathbf{432}523243$, $Y = \mathbf{52}324232523243$, $Z = \mathbf{32}432523243$.

These and variations stem from Rules 1 and 2.

Triplicate Rule

Given three operation numbers M, N and P, there are numbers X, Y, Z such that $X \to M(Y)$, $Y \to N(Z)$, $Z \to P(X)$.

Craig's 2^{nd} Law: There is an X, $X \to M(AY)$. Recall, $X = M32AM3$.

Let $A = N2P2$. Then, $X = M32N2P2M3$, $Y = N2P2X$.

So, $X \to M(Y)$.

Let $Z = P2X$. Then, $Y = N2Z$, or $Y \to N(Z)$ and $Z \to P(X)$.

So, $Z = P2M32N2P2M3$ and $Y = N2P2M32N2P2M3$.

Example: There are numbers X, Y, Z such that $X \to \overleftarrow{Y}$, $Y \to ZZ$, $Z \to X2X$.

Then, $M = 4, N = 5, P = 3$ and we have
$X = 432523243$, $Y = 5232432523243$, $Z = 32432523243$.

Ch 12. Interlude - Generalizations

The author steps in with generalizations as many mathematicians like to generalize others' work.

Observed that with Rule 4 (repetition), do not need Rule 2 (associate).

Can prove new sets of rules. The Craig and Fergusson rules hold.

Noted Facts:

Fact 1: Any machine obeying Rules 1 and 4, obeys McCulloch's Law.

Fact 2: Any machine obeying McCulloch's Law also obeys Craig's laws.

Fact 3: Any machine obeying both Craig's 2^{nd} Law and Rule 1, must obey Fergusson's Laws.

Ch 13: The Key to the Monte Carlo Lock

Craig returns from a case and meets McCulloch and Fergusson. They have a new machine with new rules.

M-I: For any X, $2X2 \to X$.

M-II: If $X \to Y$ $6X \to 2Y$.

M-III: If $X \to Y$ $4X \to \overleftarrow{Y}$.

M-IV: If $X \to Y$ $5X \to YY$.

It has many properties. Craig has difficulty finding X such that $X \to X$. One needs all four rules this time! - He thinks some more and realizes this solves the Monte Carlo Lock Problem.

He knew from the Farkus property *sp*, that the code did not specify $x \neq y$, so allowing $x = y$, or $x \to x$, it says "If x jams lock, x is neutral, if x is neutral, x jams the lock." Since this is not possible, then x has to open the lock. So, we need to find x such that $x \to x$.

The Key

The end result is that finding the combination is analogous to finding a number that produces itself in McCulloch's last machine.

We need to match letter of the code to numbers. Write Farkus' conditions using numbers where $Q = 2$, $L = 6$, $V = 4$, $R = 5$, where $x \to y$ means y is specially related to x.

So, if $y \to x$

- Q: $x \to 2x2$.
- L: $2y \to 6x$,
- V: $\overleftarrow{y} \to 4x$,
- R: $yy \to 5x$.

So, what number reproduces itself in the new machine?

The Code

M-I: For any X, $2X2 \to X$.

M-II: If $X \to Y$, $6X \to 2Y$.

M-III: If $X \to Y$, $4X \to \overleftarrow{Y}$.

M-IV: If $X \to Y$, $5X \to YY$.

We seek a number that produces itself.

Find H such that if $X \to Y$, $HX \to Y2Y2$

If so, then $H2Y2 \to Y2Y2$ since $X = 2Y2 \to Y$ by M-I.

If $Y = H$, then $H2H2 \to H2H2$.

How do we get $Y2Y2$ from given Y?

Reverse: $\overleftarrow{Y}$.

Add $2: 2\overleftarrow{Y}$.

Reverse, $Y2$.

Repeat, $Y2Y2$.

Then, $H = 5464$ and $N = H2H2 = 5464254642$. Thus, RVLVQRVLVQ.[3]

[3] $Q = 2,\ L = 6,\ V = 4,\ R = 5.$

Verificaton of Code: RVLVQRVLVQ.

Recall Farkus' Rules: For codes x and y, the following are true:

- Q: $x \to QxQ$.
- L: If $y \to x$, then $Qy \to Lx$,
- V: If $y \to x$, then $\overleftarrow{y} \to Vx$,
- R: If $y \to x$, then $yy \to Rx$.

Apply to the code:

$RVLV \to QRVLVQ$, Rule Q.

$VLVR \to VQRVLVQ$, Rule V.

$QVLVR \to LVQRVLVQ$, Rule L.

$RVLVQ \to VLVQRVLVQ$, Rule V.

$RVLVQRVLVQ \to RVLVQRVLVQ$, Rule R.

Therefore, this code is specially related to itself.

Is the Code Unique?

Makay, Géza. (2016). All Solutions of the Mystery of the Monte Carlo Lock. Found several codes of length 10-19. General forms were found. For example,

$V^kRV^\ell LV^mQV^kRV^\ell LV^mQ$ for an even k and odd ℓ and m odd.

This can be verified applying similar rule ordering as before:

$V^kRV^\ell LV^m \to QV^kRV^\ell LV^mQ$, Rule Q
$V^mLV^\ell RV^k \to V^mQV^kRV^\ell LV^mQ$, Rule V
$QV^mLV^\ell RV^k \to LV^mQV^kRV^\ell LV^mQ$, Rule L
$V^kRV^\ell LV^mQ \to V^\ell LV^mQV^kRV^\ell LV^mQ$, Rule V
$V^kRV^\ell LV^mQV^kRV^\ell LV^mQ \to RV^\ell LV^mQV^kRV^\ell LV^mQ$, Rule R
$V^kRV^\ell LV^mQV^kRV^\ell LV^mQ \to V^kRV^\ell LV^mQV^kRV^\ell LV^mQ$, Rule V

Similarly, there are codes of the form $V^mLV^kRV^\ell QV^mLV^kRV^\ell QQ$, for k even and ℓ odd.

Kovács, Zoltán Hudi, István. (2007). Brute force on 10 letters. *Teach. Math. and Comp. Sci.* 5. 183-193. Verified second 10 letter code: *VRLVQVRLVQ*.

The Rest of the Story

In Part IV, there are 6 chapters.

Dr. Fergusson creates logic machines.

Question: What is a proof?

Need precise definition if one wants to establish that a statement is not proveable from given axioms.

A proof consists of a finite sequence of sentences obeying certain rules. Can a machine determine if a sentence is provable?

Can a statement be true but not provable?

Craig, McCulloch, Fergusson could not construct a machine.

Long before 1931 - Gödel's Incompleteness Theorem.