German Encryption: The Lorenz Cipher

The 32-Character Baudot Code represented in binary using crosses (1) and dots (0)

The Lorenz Cipher Attachment & the Lorenz Teleprinter
The Encryption and Decryption Process

Lorenz encryption

<table>
<thead>
<tr>
<th>S: 10100</th>
<th>M: 00111</th>
<th>I: 01100</th>
<th>T: 00001</th>
<th>H: 00101</th>
</tr>
</thead>
</table>

Result: SMITH + JKAIVL → CWSCI

Lorenz decryption

<table>
<thead>
<tr>
<th>C: 01110</th>
<th>W: 11001</th>
<th>S: 10100</th>
<th>C: 01110</th>
<th>I: 01100</th>
</tr>
</thead>
</table>

Result: CWSCI + JKAIVL → SMITH

Baudot Code

<table>
<thead>
<tr>
<th>Binary</th>
<th>Letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000</td>
<td>Blank</td>
</tr>
<tr>
<td>00001</td>
<td>T</td>
</tr>
<tr>
<td>00010</td>
<td>CR</td>
</tr>
<tr>
<td>00011</td>
<td>O</td>
</tr>
<tr>
<td>00100</td>
<td>Space</td>
</tr>
<tr>
<td>00101</td>
<td>H</td>
</tr>
<tr>
<td>00110</td>
<td>N</td>
</tr>
<tr>
<td>00111</td>
<td>M</td>
</tr>
<tr>
<td>01000</td>
<td>Line Feed</td>
</tr>
<tr>
<td>01001</td>
<td>L</td>
</tr>
<tr>
<td>01010</td>
<td>R</td>
</tr>
<tr>
<td>01011</td>
<td>G</td>
</tr>
<tr>
<td>01100</td>
<td>I</td>
</tr>
<tr>
<td>01101</td>
<td>P</td>
</tr>
<tr>
<td>01110</td>
<td>C</td>
</tr>
<tr>
<td>11111</td>
<td>K</td>
</tr>
<tr>
<td>11110</td>
<td>J</td>
</tr>
<tr>
<td>11110</td>
<td>L</td>
</tr>
<tr>
<td>01111</td>
<td>Figure Shift</td>
</tr>
<tr>
<td>11111</td>
<td>V</td>
</tr>
<tr>
<td>11011</td>
<td>W</td>
</tr>
<tr>
<td>10110</td>
<td>U</td>
</tr>
<tr>
<td>10111</td>
<td>X</td>
</tr>
<tr>
<td>10101</td>
<td>Y</td>
</tr>
</tbody>
</table>

XOR Truth Table

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>Y</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
The Colossus Computer

- Made with 2,500 vacuum tubes
- Wheel positions simulated using thyratron rings
- Programmable using plug panels and switches
- Processing speed: 5,000 characters/second

Tommy Flowers
Conclusion

• Shortened WWII by approximately 2 years
• Classified and destroyed
• Rebuild finished in 2008
• Goal for the write-up: To investigate & understand the internal mechanisms of Colossus in more depth

Source: The National Museum of Computing
Claude Shannon’s Information Theory

BY JI WON CHUNG
APRIL 25, 2015
Significance in Context

- Nyquist 1924 & Hartley 1928
- What is information?
- Unifying Concept
- Simple
Terms

- **Information**: #bits/symbol
  - What CAN you send, not what do you send
- **Entropy**: quantitative measure of information uncertainty
- **Communication**: transmission of info across space and time
- **Channel Capacity**: how much info can be sent
- **Source Coding Theorem**: number of bits needed to send the message without much distortion
- **Channel Coding Theorem**: error reduced if info rate is < channel capacity
Fig. 1. — Schematic diagram of a general communication system.
Impact

- Coding theory
- Issues of Transactions on Information Theory
- 1970s revival
- Determined digital communication:
  - Data compression
  - Data encryption
  - Data correction
An Introduction to C Programming

CSC 103
Hannah Kwon
April 25, 2016
A BRIEF HISTORY

● Was formulated in early 1970s by an American computer scientist, Dennis Ritchie, who worked at Bell Labs (AT&T)

● Ritchie started off trying to make new file system → an intricate system called UNIX, all written through assembly language

● Its “predecessor” → B (devised in 1969~1970 by another computer scientist named Ken Thompson)

● B had its pros → was efficient and was an upgrade from assembly language

● However, it also had its cons: Thus, B → C
HOW DOES C WORK?

- C is a “compiled language”
- After writing the program, it gets run through a C compiler → changes programs into “executable”
- C itself: “human-readable” form
- “Executable” : “machine-readable” form

OTHER IMPORTANT USES:

- Operating systems
- Databases
- Interpreting language
EXAMPLE OF A C PROGRAMMING CODE

- "Include" Line: standard in & standard out
- Int: Integers
- "Main" Line
- Printf- Output
- Return 0- Make sure no error
CONCLUSION & FUTURE RESEARCH

• Why is C programming so important?
  ★ Crucial advance in the field of computer science
  ★ composes of the most basic building blocks
  ★ leads the way for C++ and future programming languages

• Paper Topic
  ★ Potential future prospects of C language
  ★ More in-depth history- how programming has evolved over time
  ★ Explain how to interpret harder C programming codes
REFERENCES

- http://computer.howstuffworks.com/c.htm
- https://www.le.ac.uk/users/rjm1/cotter/page_05.htm
- https://www.codingunit.com/the-history-of-the-c-language
- https://lh3.googleusercontent.com/3gI9l3yQynt2cj1MFdTZbaYE0VK056slvE4iejCCZQ1_-S8v3ZGDCPsIhtQsOB8Kb8i=w300
- http://s.hswstatic.com/gif/c-compile.gif
Pioneering Women in Computer Science

Tasha Binkowski

4/25/16
Narrowing Focus

ADA LOVELACE
1815-1852
First Conceptual Programmer

GRACE HOPPER
1906 - 1992
Higher-level Programming Languages

RADIA PERLMAN
Born 1951
Developed Algorithm behind STP
What is it?

→ Spanning Tree Protocol:

- Layer 2 (Data Link) protocol where bridges are used to interconnect multiple LANs (WAN) or parts of one LAN.
- Passes data back and forth to find out how the switches are organized on the network.
- Takes all the information it gathers and uses it to create a logical tree:
  - The bridges exchange information so that only one of them will handle a given message that is being sent between two computers within the network.
  - Prevents the condition known as a bridge loop.
Spanning Tree Protocol Example

Preventing Loops & Providing Path Redundancy by Creating a Tree and Only Allowing One Active Path at a Time
Conclusion

There really are too many to list
What is DNA Computing?

DNA Computing is the use of biological molecules to execute computations. In other words, it is the use of DNA molecules to encode the instructions for a computer to perform tasks with.
How does DNA Computing work?
Instructions encoded in A G C T genetic alphabet (as opposed to binary)
Because DNA strands are read in order, instructions will be read in order

Size: allows for more storage

Logic gates: can take in multiple fragments of DNA to create output
Why is DNA Computing important?

**Speed**

There is a limit on how fast electronic computers can work.

**Parallel processing**

DNA can process multiple things at once.
Sources


http://www.exploredna.co.uk/dna-computing-benefits.html


http://computer.howstuffworks.com/dna-computer.htm

http://www.britannica.com/technology/DNA-computing
DNA Computing:

- Invented by Leonard Adleman in 1994 at the University of Southern California
- Combines DNA, biochemistry, and molecular biology hardware to solve complex problems (the first one solved was the seven point Hamilton Path Problem) and comes away with multiple solutions
- Connected with Turing machines

![The logic of DNA computing](image)

The inputs to an XOR logic gate are two complementary strands of DNA. If one or the other is present, the gate fluoresces, indicating an output of 1. If both are present, they bind together preventing fluorescence, indicating an output of 0.
The Technicalities:

DNA computing works because DNA has its own coding mechanism (4-key components of the DNA molecule, storing genetic “codes”)

Enzymes react with strands of DNA and cause chain chemical reactions

Theoretically, computers using DNA computing would have much faster data transfer speeds and hold more memory

Right now, DNA computing can take hours or days, but it can make “a high amount of multiple parallel computations” (different possible solutions are created simultaneously)
Conclusion:

Since Adleman’s first proposal, many developments in the field have been made.

Scientists are still researching more efficient ways of using the technology.

Still a long way to go before it is on the market.
Sorting Algorithms
What Is Sorting?

• Sorting is ordering a list of objects so that they are organized in desired ways efficiently.

• Internal sorting
  • takes place in the main memory, where we can take advantage of the random access nature of the main memory

• External sorting
  • is necessary when the number and size of objects are prohibitive to be accommodated in the main memory.
Internal Sorting

- Bubble Sort
- Insertion Sort
- Selection Sort
- Shell Sort
- Quick Sort
- Heap Sort
External Sorting

• Mergesort
• Radix Sort
• Polyphase Sort
## Comparison of Efficiency

### Array Sorting Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Best</th>
<th>Average</th>
<th>Worst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quicksort</td>
<td>$O(n \log(n))$</td>
<td>$O(n \log(n))$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Mergesort</td>
<td>$O(n \log(n))$</td>
<td>$O(n \log(n))$</td>
<td>$O(n \log(n))$</td>
</tr>
<tr>
<td>Timsort</td>
<td>$O(n)$</td>
<td>$O(n \log(n))$</td>
<td>$O(n \log(n))$</td>
</tr>
<tr>
<td>Heapsort</td>
<td>$O(n \log(n))$</td>
<td>$O(n \log(n))$</td>
<td>$O(n \log(n))$</td>
</tr>
<tr>
<td>Bubble Sort</td>
<td>$O(n)$</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Insertion Sort</td>
<td>$O(n)$</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Selection Sort</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Shell Sort</td>
<td>$O(n)$</td>
<td>$O(n \log(n) \times 2)$</td>
<td>$O(n \log(n) \times 2)$</td>
</tr>
<tr>
<td>Bucket Sort</td>
<td>$O(n+k)$</td>
<td>$O(n+k)$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Radix Sort</td>
<td>$O(nk)$</td>
<td>$O(nk)$</td>
<td>$O(nk)$</td>
</tr>
</tbody>
</table>
Conclusion

• Investigate more about different types of sorting

• & more about the comparison of efficiency

• How do they react differently to different situations

• Efficiency: not only time but also space complexity
Assembly Language

By Dardalie Brooks
CSC103_Spring 2016
- Assembly is a “low-level” machine language.
- Machine code details instructions carried out by the CPU (processor).
Addressing Modes

Example declarations:

```
.DATA

var DB 64 ; Declare a byte, referred to as location var, containing the value 64.
var2 DB ? ; Declare an uninitialized byte, referred to as location var2.
   DB 10 ; Declare a byte with no label, containing the value 10. Its location is var2 + 1.
    X DW ? ; Declare a 2-byte uninitialized value, referred to as location X.
    Y DD 30000 ; Declare a 4-byte value, referred to as location Y, initialized to 30000.
```

- Directives (DB, DW, DD) are used to declare static data regions. They declare one, two, and four byte data locations, respectively
- **static variable** is a variable whose "lifetime" extends across the entire run of the program.
Adding a series
WHEN X= 1 and Y =5

MOV A, [x]  
Copy value of x into A

MOV B, [y]  
Copy value of y into B

.loop:  
ADD A,B  
This line says “Add B to A”

ADD B,1  
This line says “Add 1 to B”

CMP A, 15  
This line says “compare A to 15; Sets zero (Z) flay to 1 (true) when A= 15

JNZ .loop  
This line tells program to stop when Z flay = 1 ( above is true)

x: DB 0  

y: DB 1  
DB’s tell us where x and y start
Assembly in my near future

- Pros and Cons of Assembly
- Assembly beyond an introductory comp. sci. class?
- Assembly code → assembler → machine code → CPU
Citations:


2. Cutajar, John, “Intermediate 8086 Assembly Language programming,” (Slideshow presented as part of a class at the University of Malta junior College, March 17, 2012).


BACKGROUND

Classification of Robots:
1. Supervisory
2. Telesurgical
3. Shared-control

Advantages:
1. Magnification
2. No tremors
3. 3-D Vision
4. Larger range of motion
5. Ergonomically better for surgeons

Disadvantages:
1. Expenses
2. No tactile feedback
3. Less flexibility with positioning
THE DA VINCI SYSTEM

Hardware:
1. Surgical Cart
2. Vision Cart
3. Surgeon Console

How is it Used?
- Minimally Invasive Surgeries
- Training for Techniques
- Many types of surgeries
THE DA VINCI SYSTEM

How it Works:
- EndoWrist Instruments:
  - Range of Freedom
  - Motion and Flexibility
  - Small Incisions vs. Open Surgery
- Vision:
  - Uses a two channel endoscope
  - Cannot see the rest of the operating room

Technical Difficulties:
- Recoverable vs. Non-recoverable Errors
I am hoping to look into a specific surgery that surgical robots are used in, such as pancreatic surgery.

There are also different robotic systems used in surgeries that I want to investigate, such as ZEUS.
CITATIONS


Endowrist Picture from: [www.birminghambowelclinic.co.uk](http://www.birminghambowelclinic.co.uk)

ZEUS Picture from: [www.prweb.com](http://www.prweb.com)
Cloud Computing

Echo Zhang

04/25/2016

CSC 103
What is Cloud Computing and how does it work?
Why is it popular?

- Scalability
- Instant
- Save Money
Disadvantages of Cloud Computing

• Privacy
• Security
• Control
• Internet Access
Conclusion...
The History of Statistical Computation

JULIANNA CALABRESE
APRIL 25TH, 2016

“The utmost confusion is caused when people argue on different statistical data.”
–Winston Churchill
Statistics is “the science of collecting, analyzing, and interpreting numerical data relating to an aggregate of individuals.”

- First used for population and trade purposes
- Computers propelled statistical advancement
- Punch card tabulators were invented in 1890; had widespread use by the 1920s
- In U.S., the first statistical work was done in small labs
  - University of Michigan
  - Iowa State College
    - John Atansoff, inventor of the first electronic computer
- Shift towards personal computing after WWII
The Rise of Statistical Software

- 4 most used statistical programs in scholarly articles: SPSS, SAS, R and Stata
- My technical aspect: R
  - Developed by University of Auckland in 1993
    - Ross Ihaka & Robert Gentleman
  - “Data manipulation, calculation, and graphical display”
  - Open source project & completely free
  - Command-line interface
  - Both a language and an environment
  - Large user community; user-created libraries & packages
I scream, you scream...

What's your favorite flavor of ice cream?

---

```r
colors = c("brown", "pink", "white")
histogram(datacsv$flavor, main="What's your favorite flavor of ice cream?", xlab="Flavors", ylab="Number of Students", col=colors, type="count")
```
Significance & Conclusion

- More than just ice cream flavors!
- Statistics affects all fields
- Real-word applications
  - Like psychology!
- Future directions:
  - Create new randomized variables, “color” and “number”
  - See difference between how R reacts to quantitative and categorical variables
  - Conduct analysis with it using techniques from Multiple Regression
  - Experiment with other forms of visualization
References


