# An Introduction to Esoteric Programming Languages, JSFuck and Brainfuck

By James Oswald

### Workshop Overview

- 1) Introduction to Esoteric languages
  - a) About
  - b) Whitespace
  - c) Piet
  - d) Malbolge
  - e) LOLCODE
- 2) JSFuck
  - a) About
  - b) Numbers and Booleans
  - c) Letters and Strings
  - d) Execution overview
  - e) Sample programs
- 3) Brainfuck
  - a) About
  - b) Commands
  - c) Exercises
  - d) Sample Programs & Walkthrough
  - e) Interpreters



# What Are Esoteric Programming Languages?

# **Esoteric Programming Languages**

An **Esoteric Programming Language** or "**Esolang**" is a programming language created for any reason other then practical everyday use. Some of the reasons people create the languages are for:

- Proofs of concept (Brainfuck, JSFuck, BCL)
- Jokes (Ook!, Pikachu, Whitespace, Malbolge, LOLCODE)
- Art (Piet)

# What Makes an Esolang?

Most Esolangs, like all other practical programming languages try to remain **Turing Complete** while imposing other strange rule sets around the baseline of remaining turing complete.

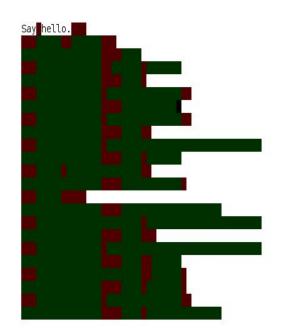
A programming language is turing complete if it can be used to solve any computational problem using a Universal Turing Machine, with no memory or speed guarantees.

# Some Esoteric Languages

# Whitespace

Whitespace is an esolang composed entirely of whitespace characters [Space], [Tab], and [LineFeed]. Because of this white space programs are invisible in normal text editors

Different combinations of these characters indicate different "instructions" and their operands, making whitespace very assembly language esque.



7,8-32

Anfang

Hello World! In Whitespace with highlighting

**Documentation** 

# Piet (Pronounced Peet)

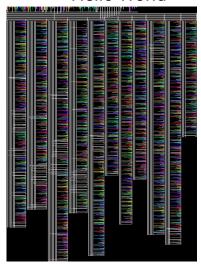
Piet is an art programming language that uses colorful bitmaps that look like modern art as programs. The language is named after Piet Mondrian who painted the original piece that inspired the language.

The Language itself is stack based and executes commands depending on colors and arrangements of blocks.

<u>Documentation</u>, <u>Program Gallery</u>



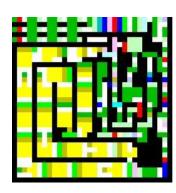
Hello World



Text Adventure Game



**Euclid's Algorithm** 



Day of the Week Calculator

# Malbolge (Pronounced mal-bulge)

Malbolge is an esolang created to be the most ungodly difficult language to program in.

- It uses base 3 numbers of length 10 rather than bytes
- The operation performed is determined as Opcode=([c]+c)%94 where c is the instruction pointer
- After an operation is performed, the instruction encrypts itself making looping near impossible.
- Normal arithmetic is replaced with trit rotation and the "crazy operation" (don't ask)
- Code is represented in ascii but still loaded in as base 3 numbers of length 10.
- Hello World is (=<`#9]~6ZY32Vx/4Rs+0No-&Jk)"Fh}|Bcy?`=\*z]Kw%oG4UUS0/@-ejc(:'8dc</li>
- It took 6 years to write a 99 bottles of beer program (<u>Link</u>).

#### **Documentation**

#### LOLCODE

LOLCODE is an esolang that speaks in meme. It's the closest thing to a real programming language on this list and resembles COBOL if you look hard enough. It's also surprisingly easy to read.

Hello World

Adder

VISIBLE s KTHXBYE

HAI 1.2 CAN HAS STDIO? VISIBLE "HAI WORLD!" KTHXBYE HAI 1.2
BTW computes the sum of 2 numbers
I HAS A x
I HAS A y
I HAS A s
GIMMEH x
GIMMEH y
x IS NOW A NUMBR
y IS NOW A NUMBR
s R SUM OF x AN Y

**Documentation**, Official Site

#### A few sample instructions

LOLCODE Construct	Purpose/ Usage
BTW	It starts a single line comment.
DOWN < variable>!! <times></times>	This corresponds to variable = variable - times. Note that "times" is a wut-only language extension.
GIMMEH <variable></variable>	This represents the input statement.
GTFO	This is similar to <b>break</b> in other languages and provides a way to break out of a loop.
HAI	This corresponds to <b>main</b> () function in other languages. It is the program entry point in LOLCODE.
HEREZ <label></label>	This is another wut-only language extension and declares a label for use with SHOO
I HAS A <type> <variable></variable></type>	This declares a variable of said type.  There are three built-in types in LOLCODE:  NUMBAH (int)  DECINUMBAH (double)  WORDZ (std::string)  Note that types are a wut-only language extension.
IM IN YR LOOP	This starts an infinite loop. The only way to exit the loop is using GTFO. Corresponds to for(;;) in other languages
IZ <expr1> <operator> <expr2>?: Conditional structure</expr2></operator></expr1>	This is similar to if operator in other languages.  Operator is one of: BIGGER THAN, SMALLER THAN, SAEM AS. Note that the ? at the end is optional.
KTHX	It ends a block. Corresponds to }
KTHXBAI	This ends a program
NOWAI	This corresponds to else
PURR <expr></expr>	This prints argument on screen, followed by a newline. It is a wut-only language extension.
RELSE	This corresponds to else (if)
SHOO	This is another wut-only language extension, that corresponds to <b>goto</b> (the horror!)
UP <variable>!!<times></times></variable>	This corresponds to variables = variable + times. Here

# JSFuck

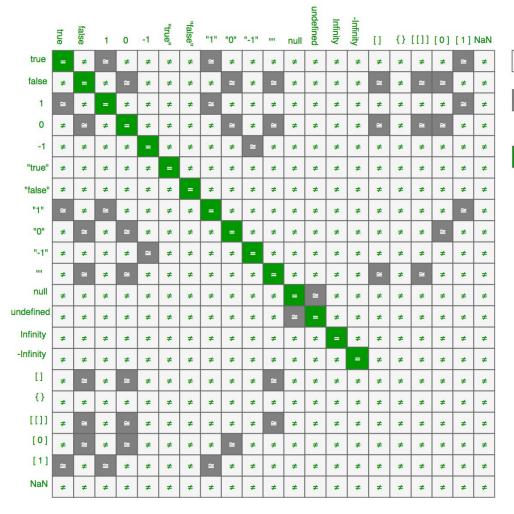
## **JSFuck**

JSFuck is a proof of concept programming language and is simply Javascript Code that only uses the six characters: []()!+

JSFuck is ALWAYS valid Javascript, it does this by taking advantage of two of Javascript's infamous design decisions, weak typing, and Javascript's nonsensical type equality system.

JSFuck is all about forcing the JS interpreter to recognize types in new ways.

Fun Fact: Any JS program can be fully converted into only JSFuck.



- ≠ Not Equal
- Loose equality
  often give false positives
  like "1" is true; [] is "0"
- Strict equality

Javascript's Insane Type Equality System

# Building valid JS code from six symbols (Numbers)

To start off, the **empty array** [], which from the last slide is **loosely equal** to 0. When applying the urinary + operator to [] we force the interpreter to recognize [] as a number type. So the expression +[] forces the interpreter to recognize [] as 0 by way of the +.

From here we use ! to force the interpreter to recognize that 0 as a boolean type meaning !+[] evaluates to true

We can use then use + to force true to evaluate to a number, +!+[] evaluates to 1

From here we use a simple pattern to build any number: !+[]+!+[] is broken up as true + true, the binary plus forces this to interpret true as a number, hence the result is 2

# Numbers and Booleans in JSF, Exercises!

Knowing that + forces numbers and ! forces booleans, we discovered +[] == 0, !+[] == true, +!+[] == 1, and !+[]+!+[] == 2

#### Solve these problems:

1) What are 3 ways we could represent false in 5 or less characters?

```
![] , !!+[] , and !!![]
```

2) How could we represent the number 3?

3) There is a way to represent 2 with only a single +, find it.

```
!![]+!![]
```

# Building valid JS code from six symbols (Strings)

We can now build any number but to write valid JS code we need letters, JSFuck uses more black magic: []+[], Binary + forces the interpreter to recognize [] as an empty string "", concatenating them as "".

Using binary + with "" we can concat the name of any type value and turn it into a string getting its letters. IE false + "" == "false" Better yet we can get "a" as (false + "")[1] expanding this with everything else we learned: (![]+([]+[]))[+!+[]]

JSFuck uses many tricks like this to get a valid combination of six symbols for every single available character.

Once we have every character we can make any string by using binary + on individual characters.

# Letters and Strings in JSF, Exercises!

```
We learned how to use the empty string []+[]== "" and used this to extract a letter from false (![]+([]+[]))[+!+[]]== (false + "")[1]== "a" Given that [][[]]== undefined and +[![]]== NaN solve these:
```

- 1) Find a representation of the string "true", use this to find "t" 
  "true" = true + "" = !![]+([]+[]) and "t" = (true + "")[0] = (!![]+([]+[]))[+[]]
- 2) Find a representation of the string "flu" (Hint: Use 'u' from undefined)

  "Flu" = "f"+"l"+"u" = (false + "")[0] + (false + "")[2] + (undefined + "")[0]

  == (![]+([]+[]))[+[]] + (![]+([]+[]))[!![]+!![]] + ([][[]]+([]+[]))[+[]]
- 3) Find a representation of the string "Nut"

```
"Nut" = "N"+"u"+"t" = (NaN + "")[0] + (undefined + "")[0] + (true + "")[0]
== (+[![]]+([]+[]))[+[]] + ([][[]]+([]+[]))[+[]] + (!![]+([]+[]))[+[]]
```

### Letters In JSFuck

USE\_CHAR\_CODE means the symbol is impossible to create in a cool way so instead uses the string \uXXX representing the unicode character and guaranteed to be creatable since u, \ and any number can be created using JSFuck.

```
'(false+"")[1]',
                                                                '(+[]+Array)[10]',
  'b':
          '([]["entries"]()+"")[2]',
                                                                                                                                 ' ': '(NaN+[]["fill"])[11]',
                                                                '(+[]+Boolean)[10]',
          '([]["fill"]+"")[3]',
                                                                                                                                       USE CHAR CODE,
                                                                'Function("return escape")()(("")["italics"]())[2]',
          '(undefined+"")[2]',
                                                                                                                                       '("")["fontcolor"]()[12]',
                                                                'Function("return escape")()([]["fill"])["slice"]("-1")', '#':
                                                         'D':
  'e':
          '(true+"")[3]',
                                                                                                                                       USE CHAR CODE,
                                                                                                                                       USE CHAR CODE.
                                                                 '(RegExp+"")[12]',
  'f':
          '(false+"")[0]',
                                                                                                                                       'Function("return escape")()([]["fill"])[21]',
                                                                 '(+[]+Function)[10]',
  'g':
          '(false+[0]+String)[20]',
                                                                                                                                       '("")["fontcolor"](")[13]',
                                                                '(false+Function("return Date")()())[30]',
                                                         'G':
  'h':
          '(+(101))["to"+String["name"]](21)[1]',
                                                                                                                                 '\'': USE CHAR CODE,
                                                         'H':
                                                                                                                                       '([]["fill"]+"")[13]',
                                                                USE CHAR CODE,
         '([false]+undefined)[10]',
  'i':
                                                                                                                                       '([0]+false+[]["fill"])[20]',
                                                         'I':
                                                                '(Infinity+"")[0]',
  'j':
         '([]["entries"]()+"")[3]',
                                                                                                                                       USE CHAR CODE,
                                                         'J':
                                                                USE CHAR CODE,
                                                                                                                                       '(+(+!+[]+(!+[]+[])[!+[]+!+[]]+[+!+[]]+[+[]]+[+[]]+[+[]])+[])[2]',
  'k':
          '(+(20))["to"+String["name"]](21)',
                                                                                                                                       '([]["slice"]["call"](false+"")+"")[1]',
                                                         'K':
                                                                USE CHAR CODE,
  '1':
          '(false+"")[2]',
                                                                                                                                       '(+(.+[0000001])+"")[2]',
                                                                USE_CHAR_CODE,
          '(Number+"")[11]',
                                                                                                                                       '(+(+!+[]+[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+[!+[]+[+[]]+[+[]])+[])[+!+[]]
                                                                 '(true+Function("return Date")()())[30]',
                                                                                                                                       '(false+[0])["italics"]()[10]',
  'n':
          '(undefined+"")[1]',
                                                                 '(NaN+"")[0]',
                                                                                                                                       '(RegExp()+"")[3]',
  '0':
          '(true+[]["fill"])[10]',
                                                                                                                                       '("")["fontcolor"](NaN+")[21]',
                                                                '(+[]+Object)[10]',
  'p':
          '(+(211))["to"+String["name"]](31)[1]',
                                                                                                                                       '("")["italics"]()[0]',
                                                         'P':
                                                                USE_CHAR_CODE,
                                                                                                                                       '("")["fontcolor"]()[11]',
         '("")["fontcolor"]([0]+false+")[20]',
                                                         '0':
                                                                                                                                       '("")["italics"]()[2]',
                                                                USE CHAR CODE,
         '(true+"")[1]',
                                                                                                                                       '(RegExp()+"")[2]',
                                                         'R':
                                                                '(+[]+RegExp)[10]',
          '(false+"")[3]',
                                                                                                                                       USE CHAR CODE,
                                                                '(+[]+String)[10]',
                                                                                                                                       '([]["entries"]()+"")[0]',
  't':
          '(true+"")[0]',
                                                                 '(NaN+Function("return Date")()())[30]',
                                                                                                                               "\\': '(RegExp("/")+"")[1]',
■'u':
          '(undefined+"")[0]',
                                                                                                                                       '([]["entries"]()+"")[22]',
                                                         'U':
                                                                 '(NaN+Object()["to"+String["name"]]["call"]())[11]',
          '(+(31))["to"+String["name"]](32)',
                                                                                                                                       USE CHAR CODE,
                                                         'V':
                                                                USE CHAR CODE,
                                                                                                                                      USE CHAR CODE,
  'W':
          '(+(32))["to"+String["name"]](33)',
                                                         'W':
                                                                USE CHAR CODE,
                                                                                                                                       USE_CHAR_CODE,
          '(+(101))["to"+String["name"]](34)[1]',
                                                                                                                                       '(true+[]["fill"])[20]',
                                                         'X':
                                                                USE CHAR CODE,
                                                                                                                                       USE_CHAR_CODE,
  'v':
         '(NaN+[Infinity])[10]',
                                                         'Y':
                                                                USE CHAR CODE,
                                                                                                                                       '([]["fill"]+"")["slice"]("-1")',
          '(+(35))["to"+String["name"]](36)',
                                                                USE CHAR CODE,
                                                                                                                                 '~': USE_CHAR_CODE
```

# **Executing JSFuck**

So far we can create JS expressions out of six symbols that evaluate to numbers and letters and strings, but in order to actually run code we need to use the **eval** function.

Eval is a built in JS function that will execute whatever string is passed as a parameter as javascript. EX. eval("console.log('hello')") prints hello to the console. However since we eval(JSFuckExpressionHere) isn't valid JSFuck in itself this would be cheating.

Thankfully there is a very creative and complex workaround to this allowing us to effectively run any string using only the symbols we have available to us.

# The Very Creative and Complex Workaround (Prototypes)

Javascript is a prototype based language, we can access any object's prototype, the prototype contains a list of properties and methods of the object's "pseudo class".

This is how JS knows if something like d.get() is legal without needing class information. The interpreter will look in the prototype of d see if ".get()" is valid and if so will run the method from the Function object reference in the prototype.

You can access an objects prototype using 'object["protoFunctionName"]'

#### **Console Demo of Prototypes**

# The Very Creative and Complex Workaround (Array Prototypes & Function Prototypes)

[] is an array object. Since [] is an Array Object we can access the Array Prototype which contains all JS's built in array methods like "push".

```
[]["push"] == f push() { [native code] }
```

Pick an arbitrary array method, this method itself has a prototype, it is a Function Object. Inside the function object prototype is the function object "constructor".

```
[]["push"]["constructor"] = f Function() { [native code] }
```

# The Very Creative and Complex Workaround (The Function Object Constructor)

We now have access to the function object constructor. The function object constructor takes a single string of JS code as a parameter and will use it as the body of a function.

```
Let f = new Function("alert('oh boy')");
```

The function Object is special in another way as well, a function object suffixed with () will be executed as a function ie:

```
new Function("alert('oh boy')")();
```

# The Very Creative and Complex Workaround (Putting it All Together)

We take the function object constructor from array.push.constructor, give it code as a parameter and tell it to execute our a function all in one by stating:

```
[]["push"]["constructor"]("alert('hello')")()
```

With this we can create the strings "push" and "constructor" and all of our code using the method to create all of our strings with JSFuck. This allows us to create and execute any Javascript program using only these 6 symbols.

The simple example from the last page:

```
[]["push"]["constructor"]("alert('hello')")() =
```

 $\frac{1}{1} \frac{1}{1} \frac{1}$ \\ \text{\color=1} \\ \text{\col and the control of th and in the first of the first o 

# A Simple JSFuck Program... Oh dear god

# But why should I care about JSFuck?

JSFuck is a great esoteric language that is made cooler by knowing every JSFuck program is valid javascript and every javascript program can be written in JSFuck. For example, looking at JQuery Skewed, it is a complete, working implementation of JQuery in JSFuck that works with any normal Javascript code. (<u>Link to JQ Skewed</u>)

JSFuck is used as a tool for hacking, and most sites aren't clever enough to check if JSFuck is valid javascript code, making it much more likely to be successfully injected without setting off anti-scripting alarms. Ebay was known to be hit with a massive JSFuck attack that allowed users to upload custom JSFuck code to their profiles. (Link to article)

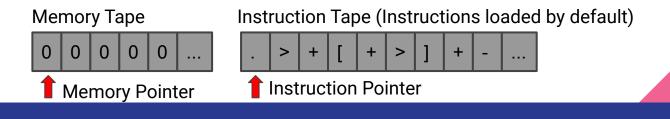
# Brainfuck

### What is Brainfuck?

**Brainfuck** is a proof of concept programming language that uses only eight symbols and is widely considered the most famous esoteric programming language, inspiring many spin-offs and copycats with its fame.

The Brainfuck machine is visualized as an infinite (or finite) tape of cells on which cells contain bytes. The machine has a pointer that points to a cell on the tape. A separate tape exists containing instructions and an instruction pointer.

A Brainfuck Abstract machine in its default state:



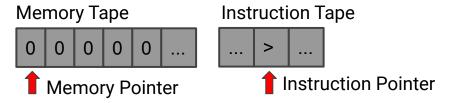
### **Brainfuck Instructions**

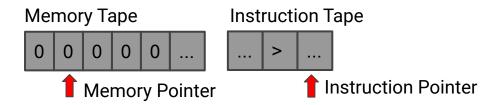
All 8 of the brainfuck instructions center around manipulating cells, the cell pointer, and the instruction pointer, the instruction tape is immutable (and hence the instructions themselves are also immutable). Let's look at the instructions and their descriptions:

>	moves the cell pointer right
<	moves the cell pointer left
+	Adds 1 to the current cell pointed to by the cell pointer
-	Subtracts 1 from the current cell pointed to by the cell pointer
	Prints the ascii value of the cell pointed to by the cell pointer
,	Reads an ascii value to the cell pointed to by the cell pointer
[	If cell pointed to by the cell pointer is 0 jump to matching ]
]	If cell pointed to by the cell pointer is not 0 jump to matching [

# > (Shift Memory Pointer Right)

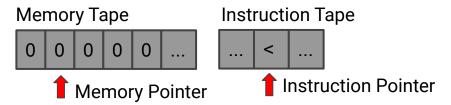
#### Before:

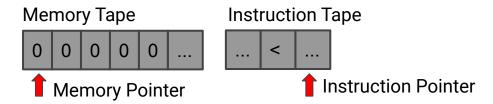




# < (Shift Memory Pointer Left)

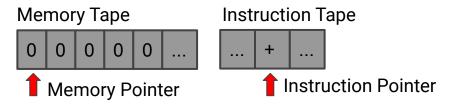
#### Before:

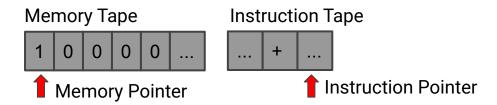




# + (Add 1 to Cell at Mem Pointer)

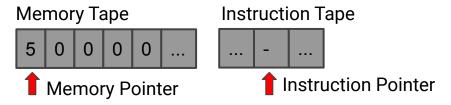
#### Before:

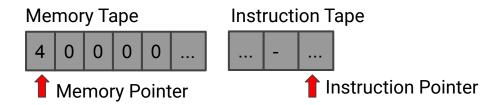




# - (Sub 1 From Cell at Mem Pointer)

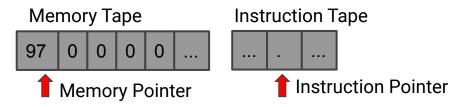
#### Before:



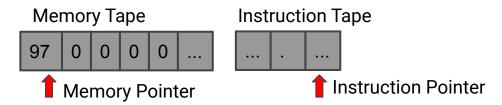


# . (Print Ascii of Cell at Mem Pointer)

#### Before:

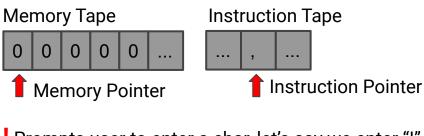


! "a" printed to the console

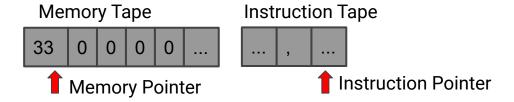


# , (Read Ascii input to Cell at Mem Pointer)

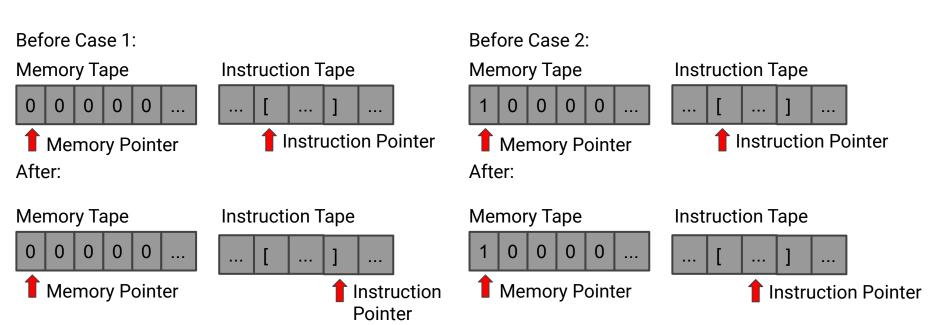
#### Before:



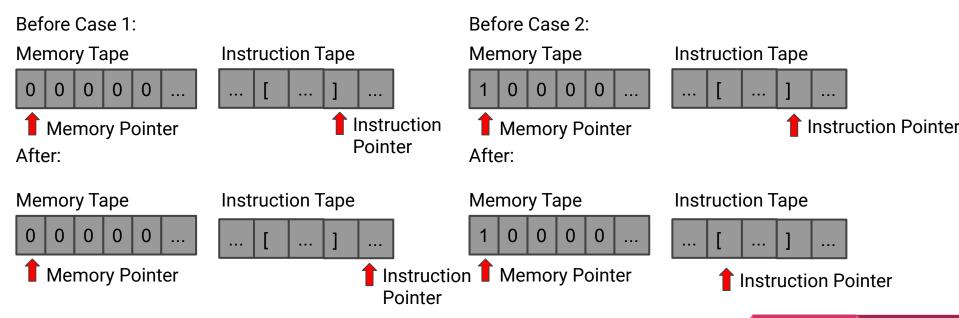
Prompts user to enter a char, let's say we enter "!"



# [ (If Cell at Mem Pointer == 0 jump to matching ])



# ] (If Cell at Mem Pointer != 0 jump to matching [)



# Brainfuck, Exercises!

Using the instruction list to the right solve:

moves the cell pointer right
moves the cell pointer left
Adds 1 to the current cell pointed to by the cell pointer
Subtracts 1 from the current cell pointed to by the cell pointer
Prints the ascii value of the cell pointed to by the cell pointer
Reads an ascii value to the cell pointed to by the cell pointer
If cell pointed to by the cell pointer is 0 jump to matching ]
If cell pointed to by the cell pointer is not 0 jump to matching [

- 1) Write a program that reads a single digit number, adds 1, then prints the number ,+. Link
- 2) Write a program that reads 3 characters then prints them out backwards ,>,>,.<.<. <u>Link</u>
- 3) Write a program that reads 3 characters then prints them out forwards ,>,>,<<.>.>. <u>Link</u>
- 4) (Challenge) Write a program that takes 2 ascii chars as bytes and adds them, and prints the resulting byte as an ascii character (Hint use a loop to add 1 to the first number and subtract 1 from the second until there is nothing left)

# Sample Program

Add two single digit numbers with a single digit result

#### An explanation

#### EX.

Say we input 3 and 4, the program will read these as ascii values into cells 1 and 2 as their ascii representations 51 and 52.

We then enter the loop which performs the addition and get, 51 + 52 = 103, in cell 1.

Cell 1 then has 48 subtracted from it, 103 - 48 = 55. Which is then printed as the ascii character 7.

Let's Step Through this on an interpreter (Click Here)

### Hello World! In Brainfuck

#### Minimized Hello World! in Brainfuck

#### An explanation

```
;initialize counter (cell 0) to 10
+++++++++
                      ;use loop to set 70/100/30/10
   >++++++
                      ;add 7 to cell 1
                     ;add 10 to cell 2
   >+++++++++
                      ;add 3 to cell 3
   >+++
                      ;add 1 to cell 4
   >+
                      ;decrement counter (cell 0)
   <<<<-
                      ;print 'H'
>++.
                      ;print 'e'
>+.
                      ;print 'l'
++++++
                      ;print 'l'
                      ;print 'o'
+++.
                      ;print ' '
>++.
;print 'W'
                      ;print 'o'
>.
                      ;print 'r'
+++.
                      ;print 'l'
                      ;print 'd'
                      ;print '!'
>+.
                      ;print '\n'
>.
```

Visualize This (Click Here)

# **Brainfuck Interpreters**

Brainfuck is an easy language to make an interpreter for, here are a few:

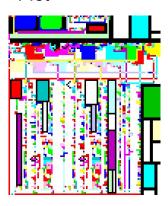
С

```
#include<stdio.h>
int d[9999],a[9999],p,l,i,c;
main(int j,char **k){
         FILE *f=fopen(k[1],"r");
         for(;(c=fgetc(f))!=EOF;i++)d[i]=c;
         for(i=0;d[i]>0;i++){}
                   if(d[i]==43)a[p]++;
                   if(d[i]==45)a[p]--;
                   if(d[i]==62)p++;
                   if(d[i]==60)p--;
                   if(d[i]==46)putchar(a[p]);
                   if(d[i]==44)a[p]=getchar();
                   if(d[i]==91&&!a[p])
                             for(I=0;i++&&d[i]!=93||I;){
                                       if(d[i]==91)I++;
                                       if(d[i]==93)I--;
                   if(d[i]==93\&\&a[p])
                             for(I=0;i--&&d[i]!=91||I;){
                                       if(d[i]==93)I++;
                                       if(d[i]==91)I--;
```

#### Brainfuck

```
>>>+[,>+++++|(----->-]<[->++++|(-|>>)|(->+>>)|
>>>>]<<[->+>+<<]>>>(->+>+<<]>>(->+>+</
>+<[>-<[-]]>[-<<[-]++++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+<[>--->]+<[>--->]+++++|<--->]+<[>--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>--->]+++++|<--->]+<[>---->]+++++|<--->]+<[>---->]++|
<<+>>>]<<+>+<[>-]>[-<->>]</+>(>-]>[-]>[-<->>]</+>(>-]>[-]>[-]>[-]>[-<--
>-->+<[>-]>[-<<->>)[>->+<[>-]>
[->;]>>]>+<<<([<<]>>)]<->+<[>-]>;[->>
[-<]>+<->>[<>>)-|</>->=
>>]>>>[>-]</-]</->>/>>/>>
<|>>|<+++++++>>>|
```

#### Piet



# Brainfuck spinoffs

Due to brainfucks popularity, It has gained a number of copycat esoteric languages. They all just replace the 8 symbols with new symbols or words. This family of esolang are called TrivialBrainfuckSubstitution languages (see here for more)

#### Ook!

Brainfuck	Ook!
>	Ook. Ook?
<	Ook? Ook.
+	Ook. Ook.
-	Ook! Ook!
	Ook! Ook.
,	Ook. Ook!
[	Ook! Ook?
]	Ook? Ook!

#### Pikalang

Brainfuck	Pikalang
>	pipi
<	pichu
+	pi
-	ka
	pikachu
	pikapi
[	pika
]	chu

#### **Alphuck**

Brainfuck	Alphuck
>	a
<	С
+	е
2	i
	j
,	0
[	р
1	s

# Thanks For Coming! Stay Around for Noor