NES CARTRIDGE

I Dream of Game Genies and ZIP Files

Hacking the NES

20 JULY 2018

PRESENTED BY VI GREY

START PRESENTATION

SPECIAL THANKS

VIGREY.COM - TWITTER.COM/@VIGREYTECH

#HOPECONF

#HOPEXII

NES CARTRIDGE

I Dream of Game Genies and ZIP Files

Hacking the NES

20 JULY 2018

PRESENTED BY VI GREY

START PRESENTATION

SPECIAL THANKS

VIGREY.COM - TWITTER.COM/@VIGREYTECH

#HOPECONF

#HOPEXII

-SPECIAL THANKS-

2600 & HOPE

CHRUTH FABIAN

THE MACHINE SHED LLC

MY FAMILY

ANGE ALBERTINI
DWANGOAC & TASBOT TEAM
EVAN SULTANIK
EVAN TERAN
GAMESDONEQUICK
NESDEV WIKI/FORUMS
TRAVIS GOODSPEED
TYMKRS

B - TITLE

NES CARTRIDGE

I Dream of Game Genies and ZIP Files

Hacking the NES

20 JULY 2018

PRESENTED BY VI GREY

START PRESENTATION

SPECIAL THANKS

VIGREY.COM - TWITTER.COM/@VIGREYTECH

#HOPECONF

#HOPEXII

NES CARTRIDGE

I Dream of Game Genies and ZIP Files

Hacking the NES

20 JULY 2018

PRESENTED BY VI GREY

START PRESENTATION

SPECIAL THANKS

VIGREY.COM - TWITTER.COM/@VIGREYTECH

#HOPECONF

#HOPEXII

-WHO AM I?-

- TECHNOLOGY RESEARCHER
- SOFTWARE ENGINEER
- WEB DEVELOPER
- CO-FOUNDED AND CO-RUNS AN INTERACTIVE TECHNOLOGY STUDIO "BLACKPAWNSTUDIOS"

[FREQUENTLY SPOTTED
SOLVING RUBIK'S CUBES]

B - PREV A - NEXT

-BEFORE WE BEGIN-

- 3 ACT PRESENTATION
- NES ROM FILE WILL BE MADE AVAILABLE
- SOURCE CODE WILL BE AVAILABLE ON GITHUB
- SLIDES WILL BE MADE AVAILABLE AS A PDF
- VIGREY.COM/HOPEXII

B - PREV A - NEXT

-BEFORE WE BEGIN (2)-

- I AM NOT AN NES EXPERT
- THE F-WORD IS USED IN TWO PROPER NOUNS
- CANNOT GUARANTEE THIS ROM OR METHODS WILL NOT DAMAGE YOUR NES

B - PREV A - NEXT

-CONTEXT-

- READ POC||GTFO 0X14 (PDF/ZIP/NES POLYGLOT)
- MADE NES CART FOR TYMKRS' HACKERSPACE
- MADE NESZIP ROM AND WROTE POC||GTFO 18:04
- MADE TBAS INTERPRETER NES CART FOR CYPHERCON

-ACT 0-

NES HARDWARE OVERVIEW

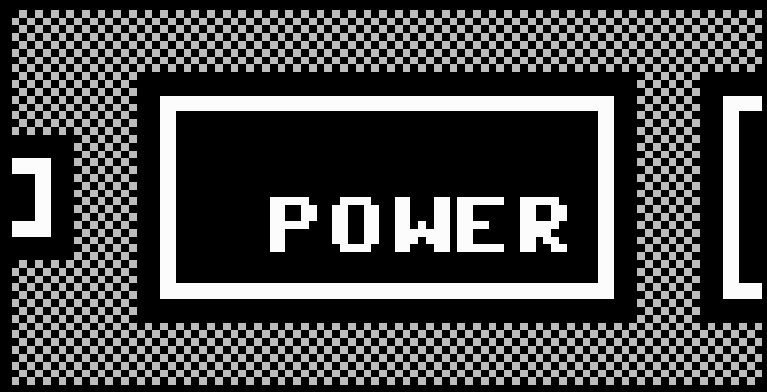
B - PREV A - NEXT

-NES CONSOLE-

PRESENTATION GOES HERE

B - PREV A - NEXT

-POWER BUTTON-

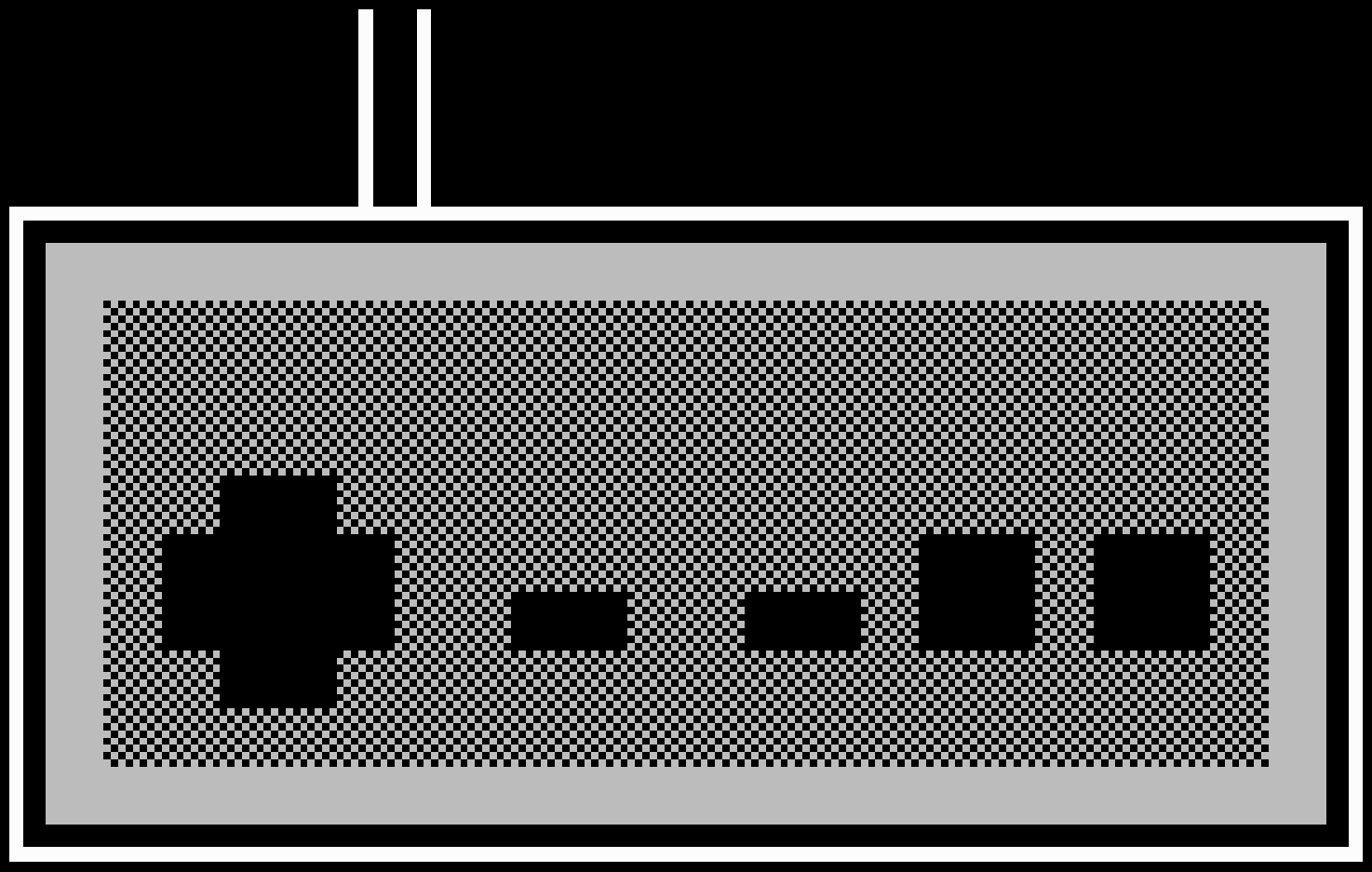


B - PREV A - NEXT

-RESET BUTTON-

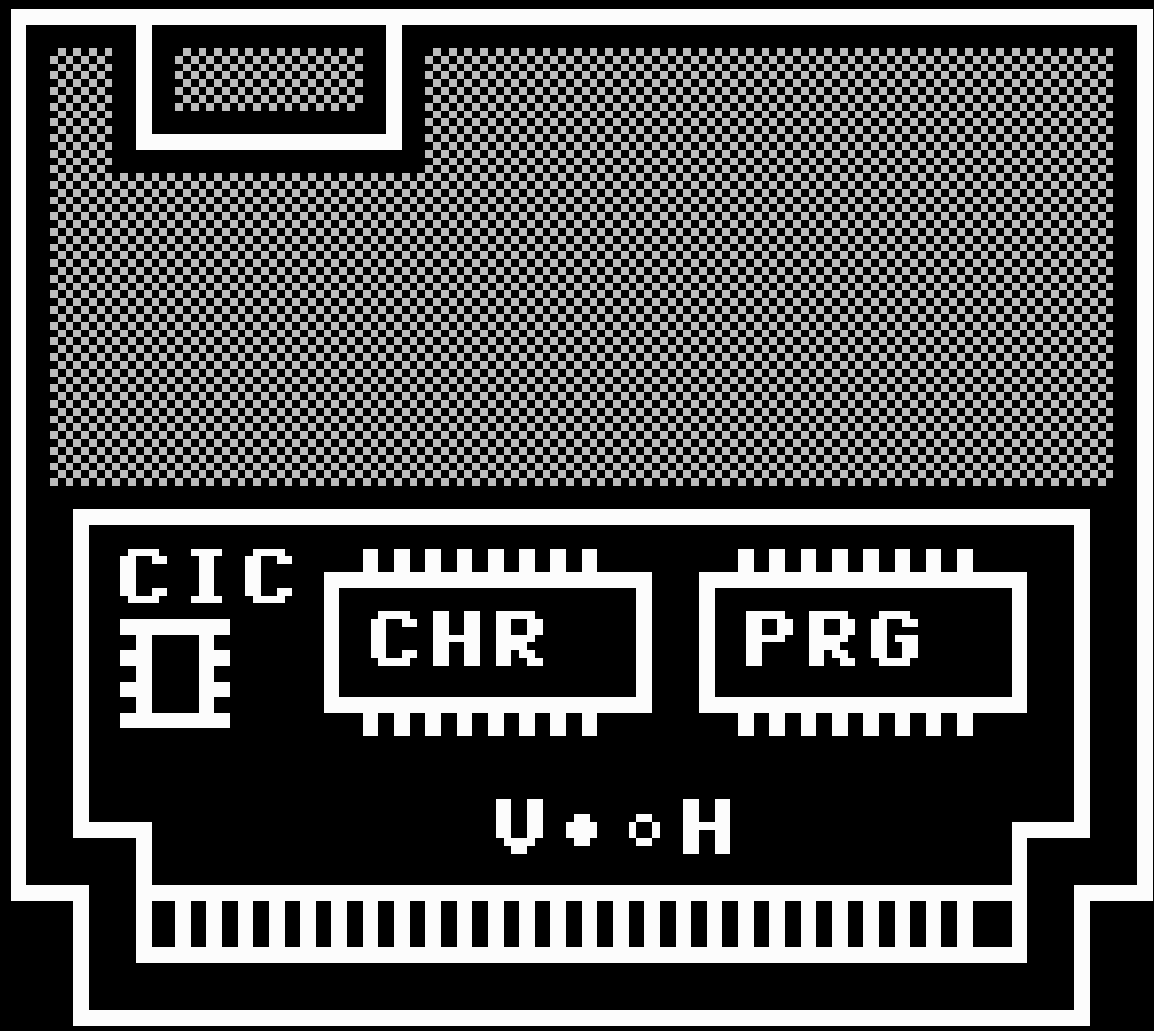
B - PREV A - NEXT

-CONTROLLER-



B - PREV A - NEXT

-NES-NROM-256 CARTRIDGE-



B - PREV A - NEXT

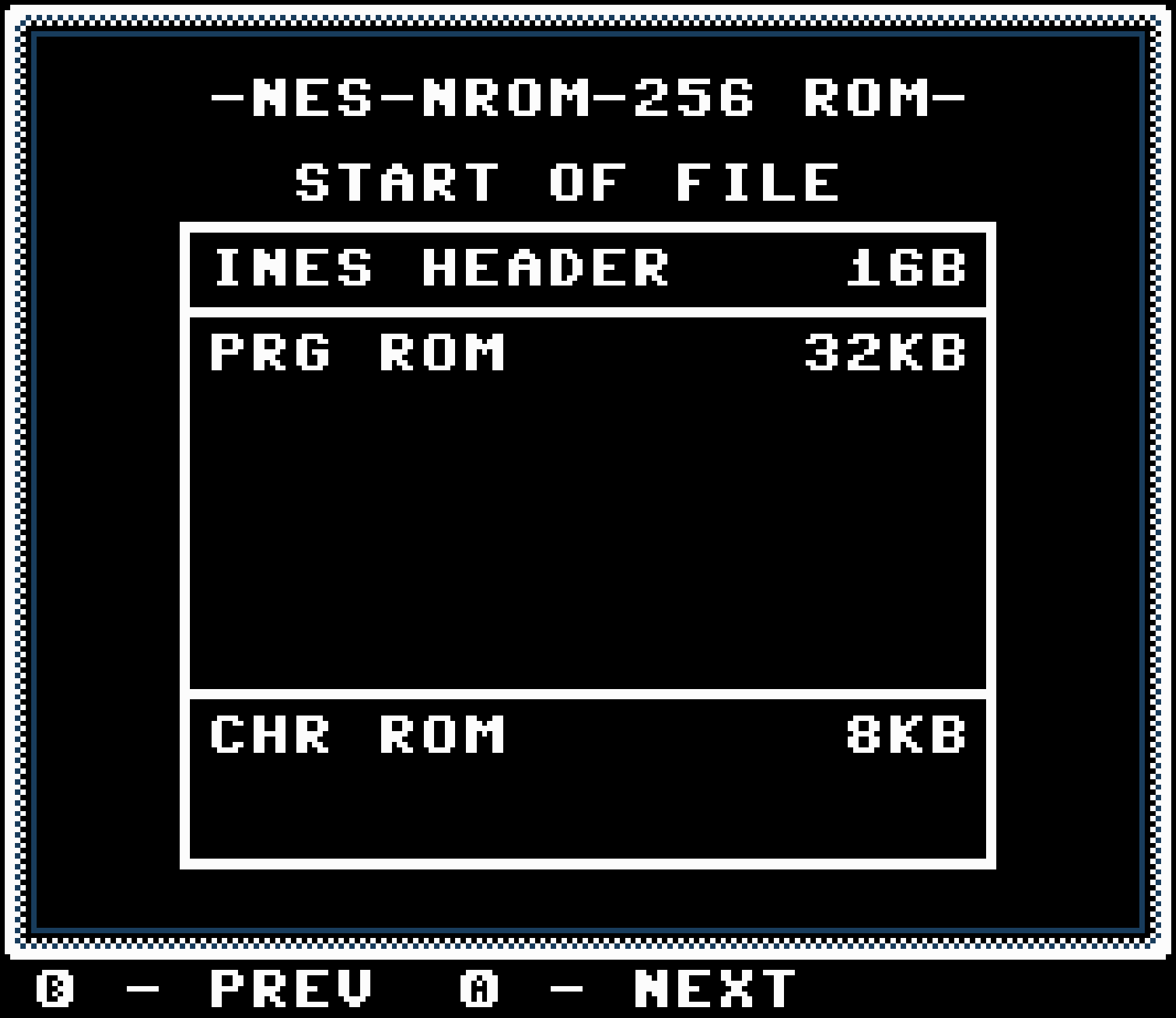
-EPROMS-

- ERASABLE PROGRAMMABLE READ ONLY MEMORY

256 KILOBITS

32 KILOBYTES

B - PREV A - NEXT


-NES-NROM-256 ROM-
START OF FILE
INES HEADER 16B
PRG ROM 32KB
CHR ROM 8KB
B - PREV A - NEXT

-CHR ROM-

◦ TILE DATA

2 X PATTERN TABLE

B - PREV A - NEXT

-PRG ROM-

- PROGRAMMING DATA
- 6502 MACHINE CODE
- TELLS THE NES CONSOLE HOW TO BEHAVE
- LAST 6 BYTES SAY WHERE PROGRAM STARTS AND WHERE IMPORTANT INTERRUPTS ARE

B - PREV A - NEXT

-INES HEADER-

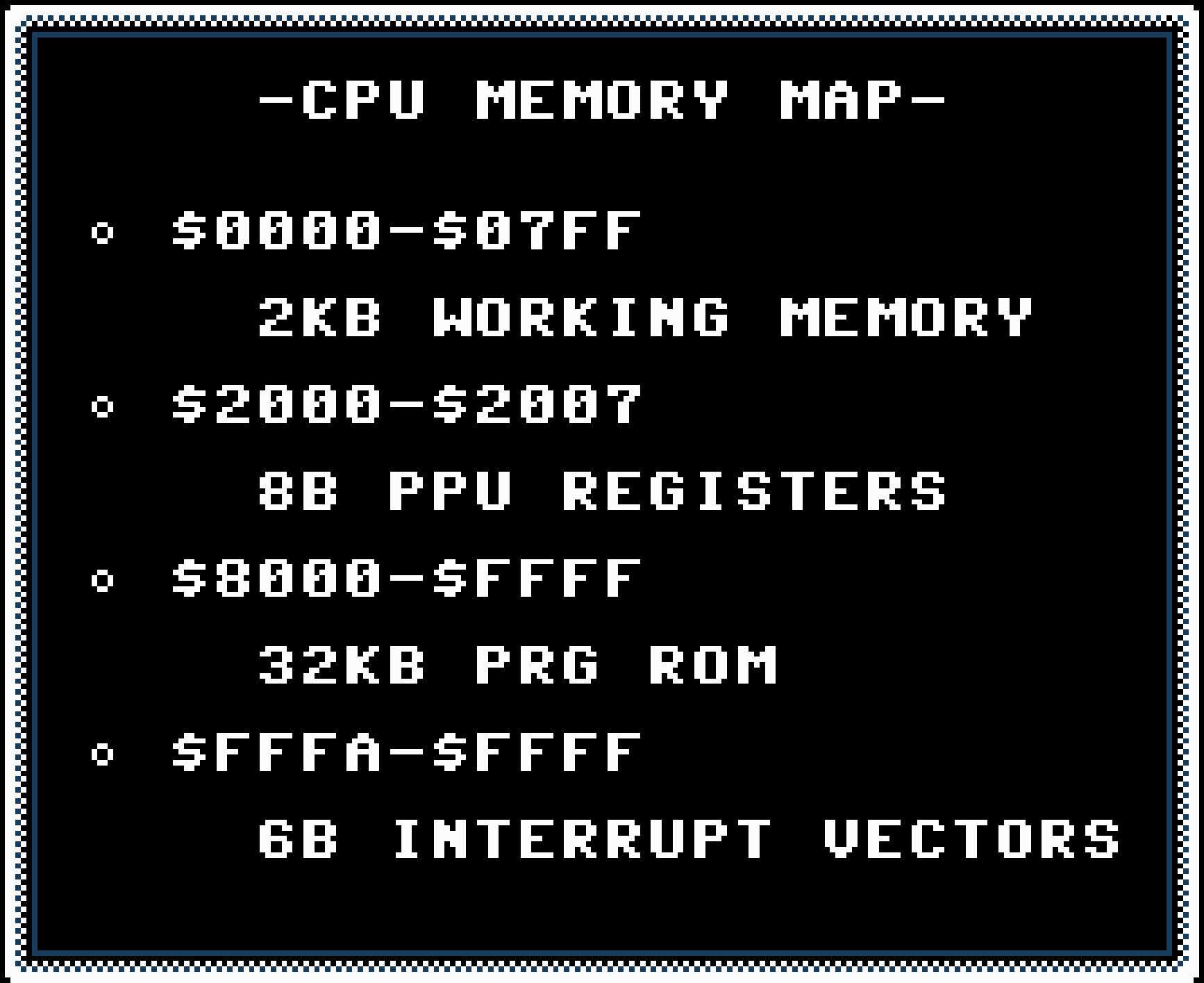
NES<1A><02><01>...

- 16 BYTE ROM HEADER
- SPECIFIES LENGTH OF CHR AND PRG ROM DATA
- TELLS EMULATORS HOW TO HANDLE NES ROM FILE
- NES<1A> - MAGIC STRING
- <02> - 2 X 16KB PRG
- <01> - 1 X 8KB CHR

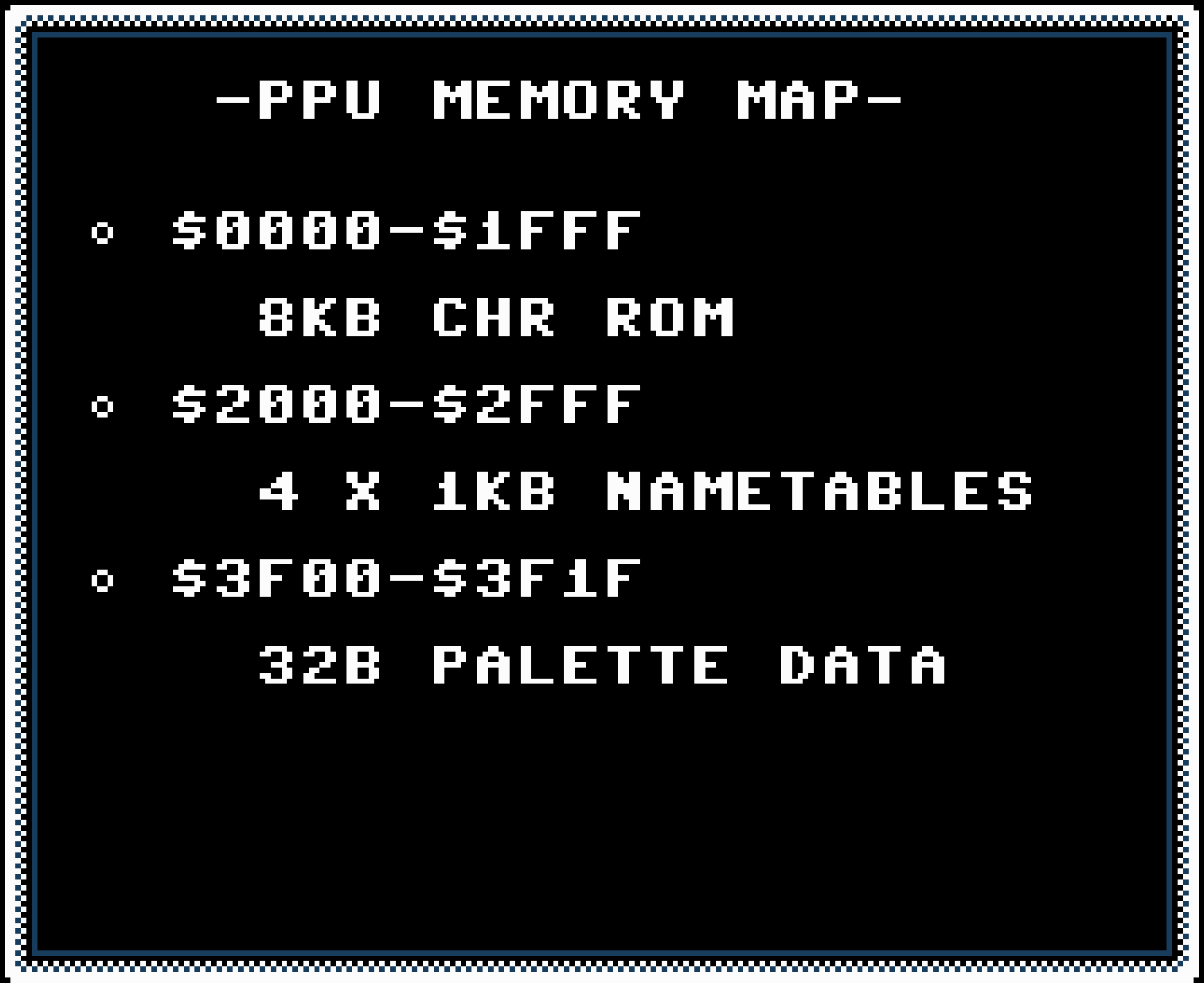
-PROCESSORS-

- CPU - CENTRAL PROCESSING UNIT (BASED ON THE 6502 MICROPROCESSOR)
- PPU - PICTURE PROCESSING UNIT
- APU - AUDIO PROCESSING UNIT

B - PREV A - NEXT


-CPU MEMORY MAP-
$0000-$07FF
2KB WORKING MEMORY
$2000-$2007
8B PPU REGISTERS
$8000-$FFFF
32KB PRG ROM
$FFFA-$FFFF
6B INTERRUPT VECTORS

B - PREV A - NEXT


-PPU MEMORY MAP-
$0000-$1FFF
8KB CHR ROM
$2000-$2FFF
4 X 1KB NAMETABLES
$3F00-$3F1F
32B PALETTE DATA

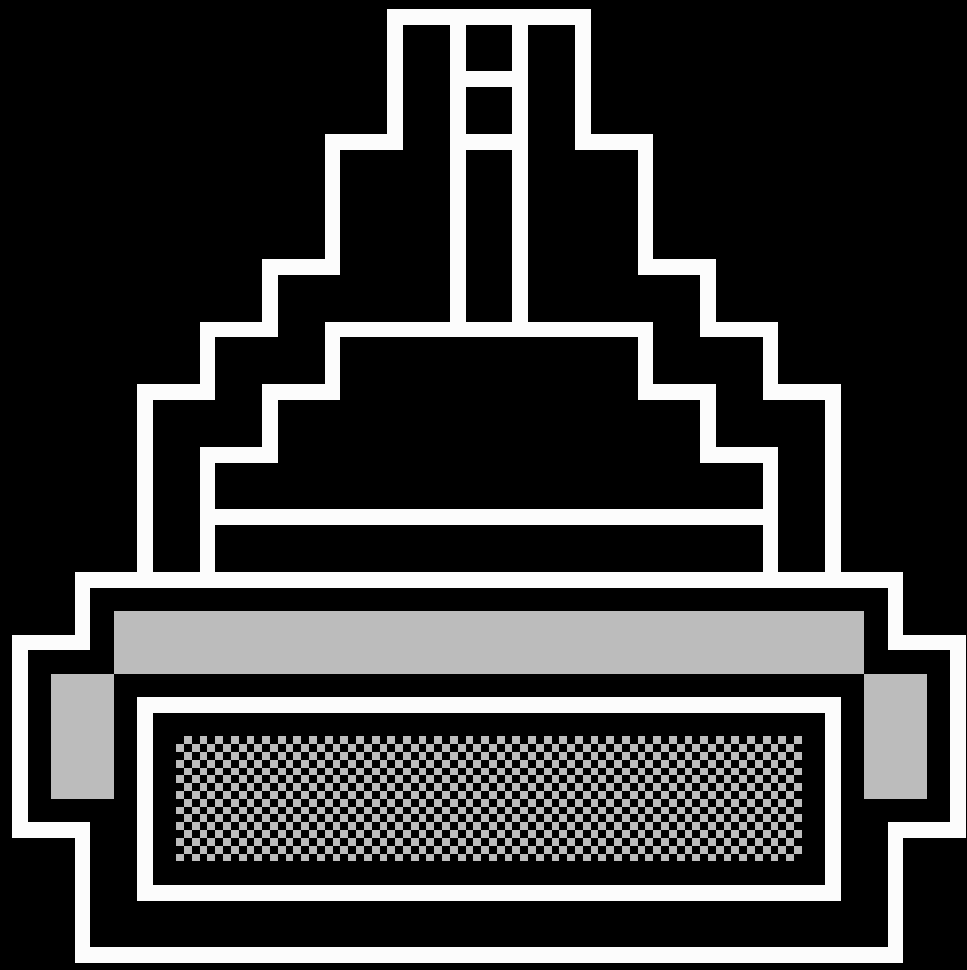
B - PREV A - NEXT

-ACT 1-

INTERACTIVITY

B - PREV A - NEXT

-GAME GENIE-

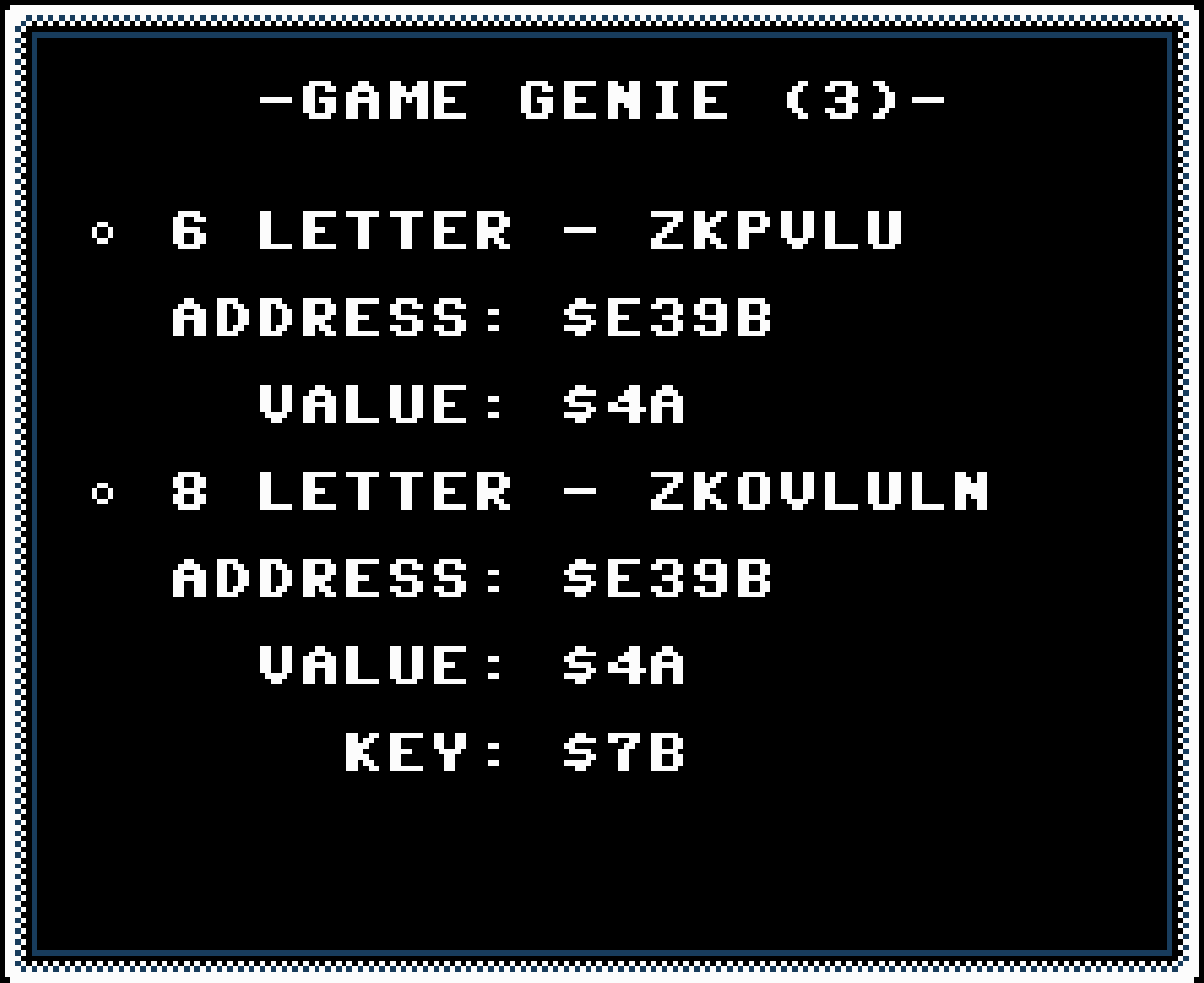


B - PREV A - NEXT

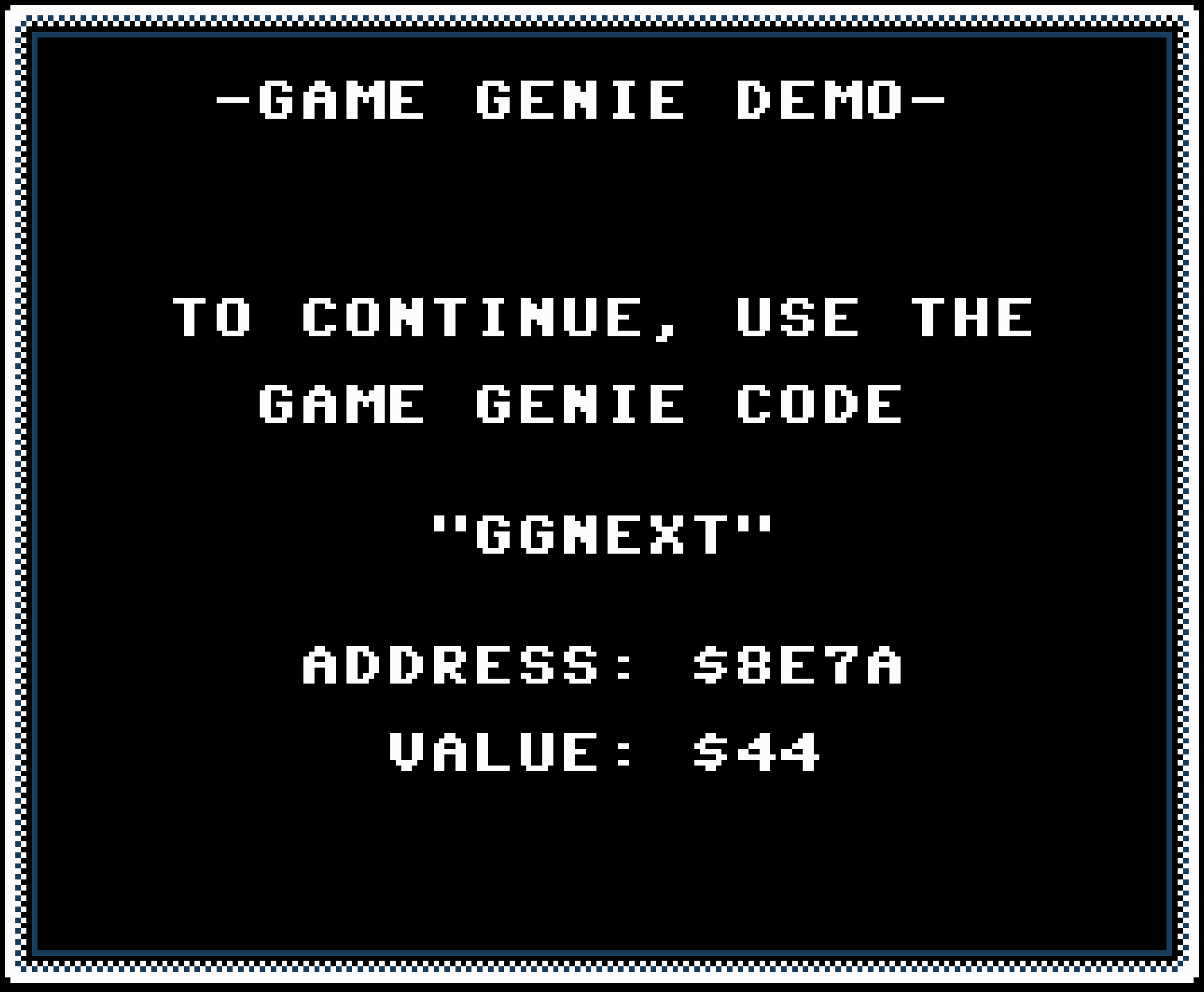
-GAME GENIE (2)-

- CHEATING DEVICE
- 6 OR 8 LETTER CODES
- A E P O Z X L U
  G K I S T V Y N
- TAKES 1 ADDRESS VALUE
  ($8000 - $FFFF)
- CHANGE VALUE BYTE
- OPTIONAL KEY COMPARE

B - PREV A - NEXT


-GAME GENIE (3)-
◦ 6 LETTER - ZKPVLU
ADDRESS: $E39B
VALUE: $4A
◦ 8 LETTER - ZKOVLULN
ADDRESS: $E39B
VALUE: $4A
KEY: $7B

B - PREV A - NEXT

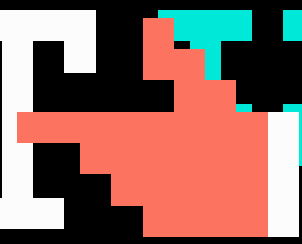


B - PREV "GGNEXT" - NEXT

Game Genie

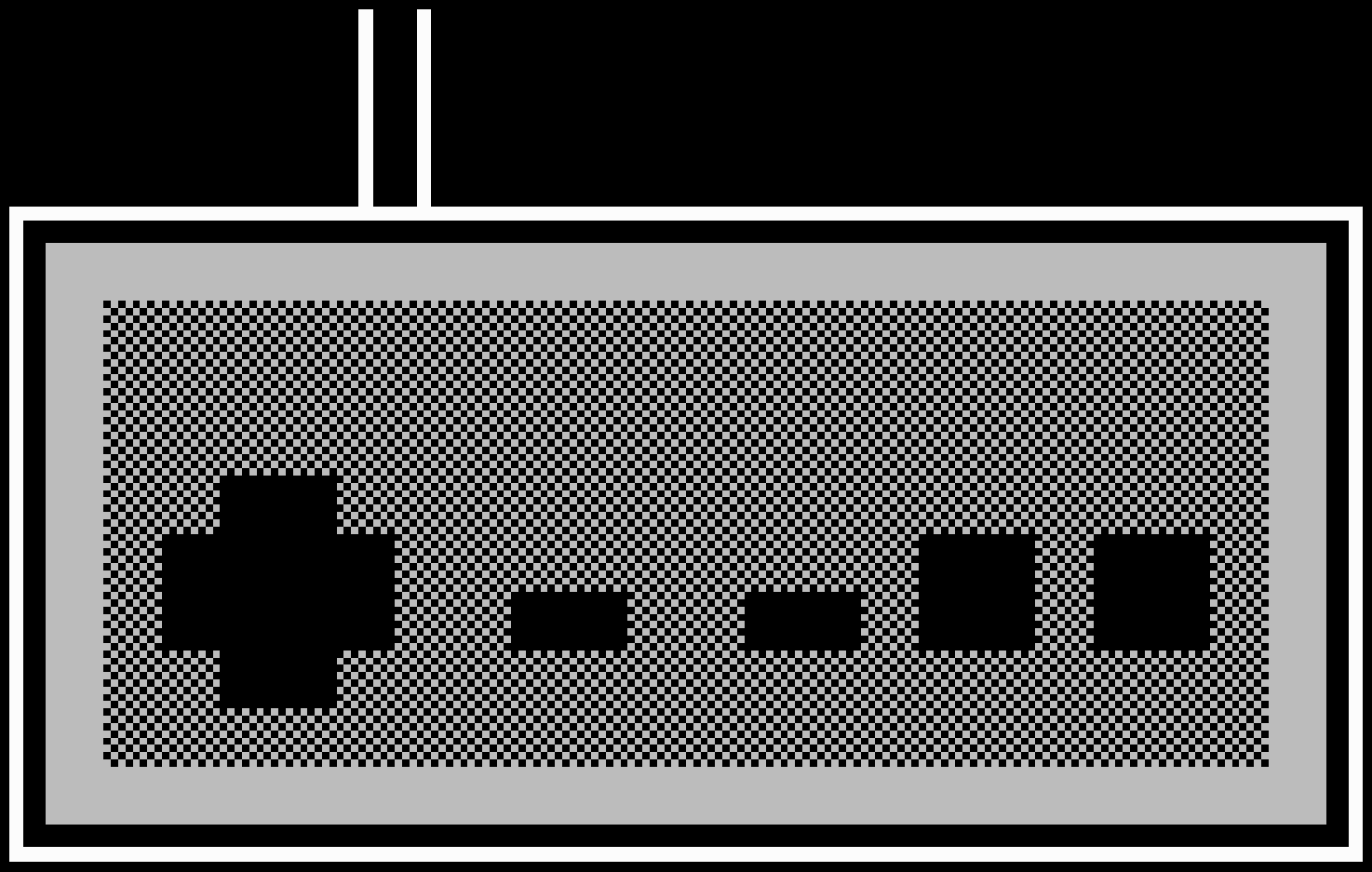
APU ZXLU

GKISTYN



GGNEXT +

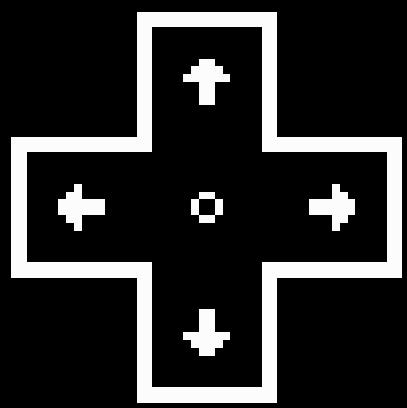
-CONTROLLER-



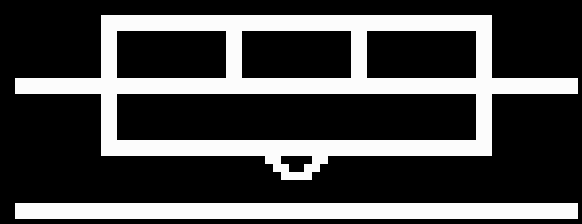
B - PREV A - NEXT

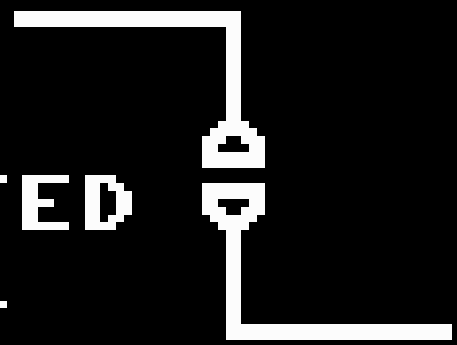
-CONTROLLER D-PAD-

BUTTON



SIDE VIEW





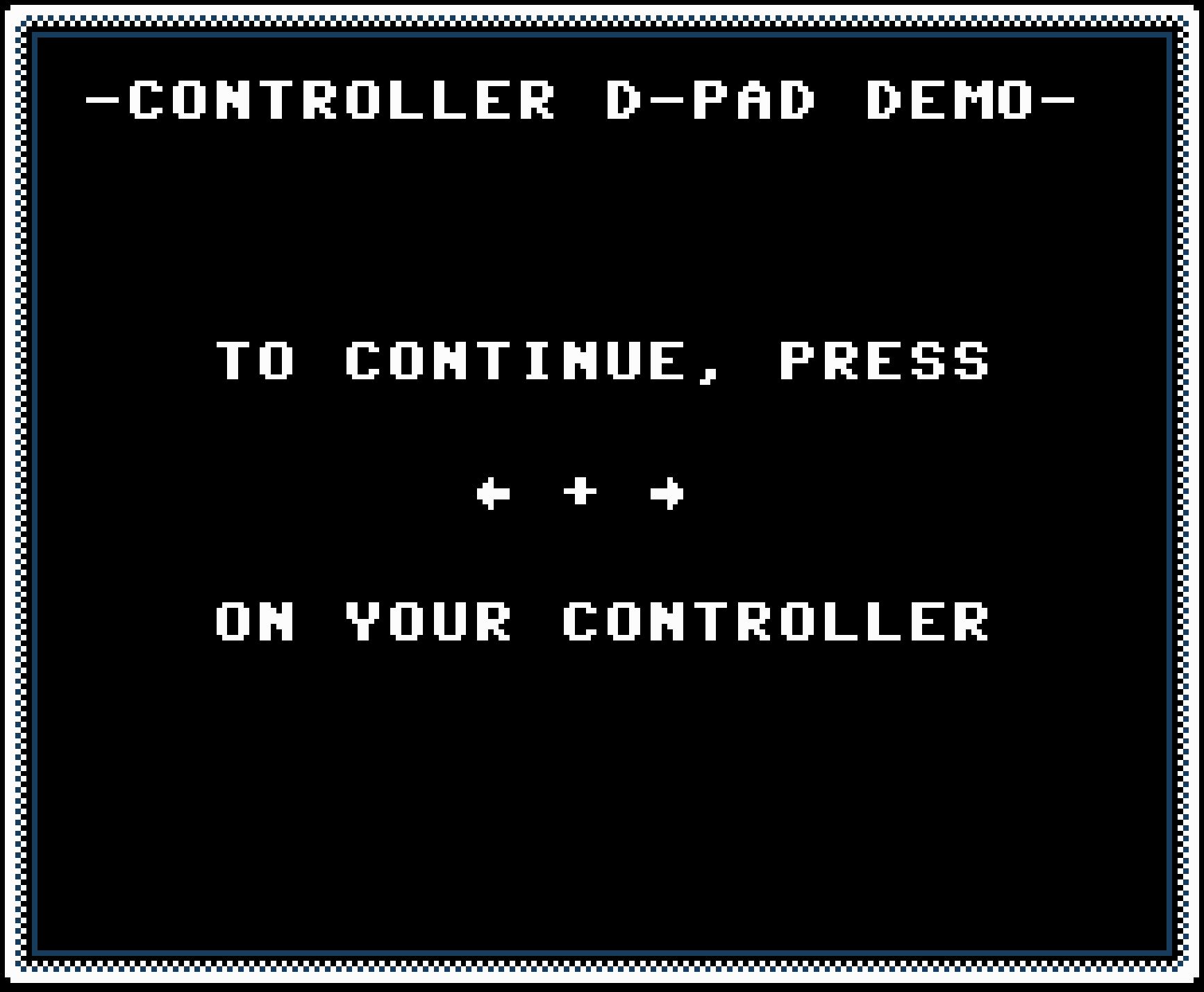
SEPARATED CIRCUIT

B - PREV A - NEXT

-CONTROLLER D-PAD (2)-

- SEESAW DESIGN OF D-PAD PREVENTS ↑+↓ AND ←+→
- CONDUCTIVE RUBBER PADS CAN STILL BE USED
- CONTROLLER CAN BE TAKEN APART

B - PREV A - NEXT



B - PREV ← + → - NEXT

-RESET BUTTON-

B - PREV A - NEXT

-RESET (2)-

- FORCES GAME TO START PROGRAM FROM BEGINNING
- DOES NOT RESET MEMORY LIKE POWER BUTTON DOES
- TO DETECT RESETS, ON PROGRAM START, CHECK IF SPECIFIED VALUES IN MEMORY ARE STILL SET

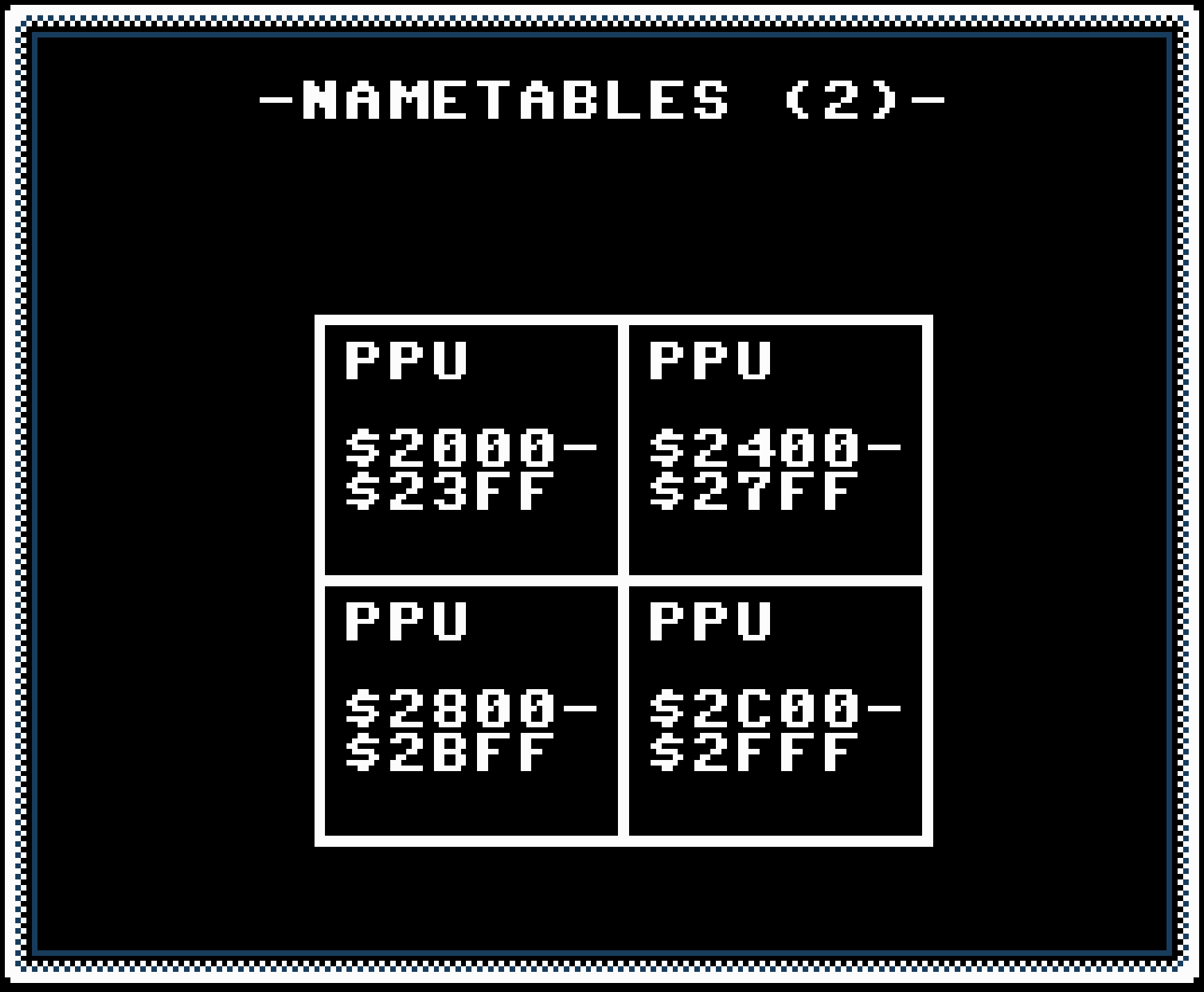
-RESET DEMO-

TO CONTINUE, PRESS THE

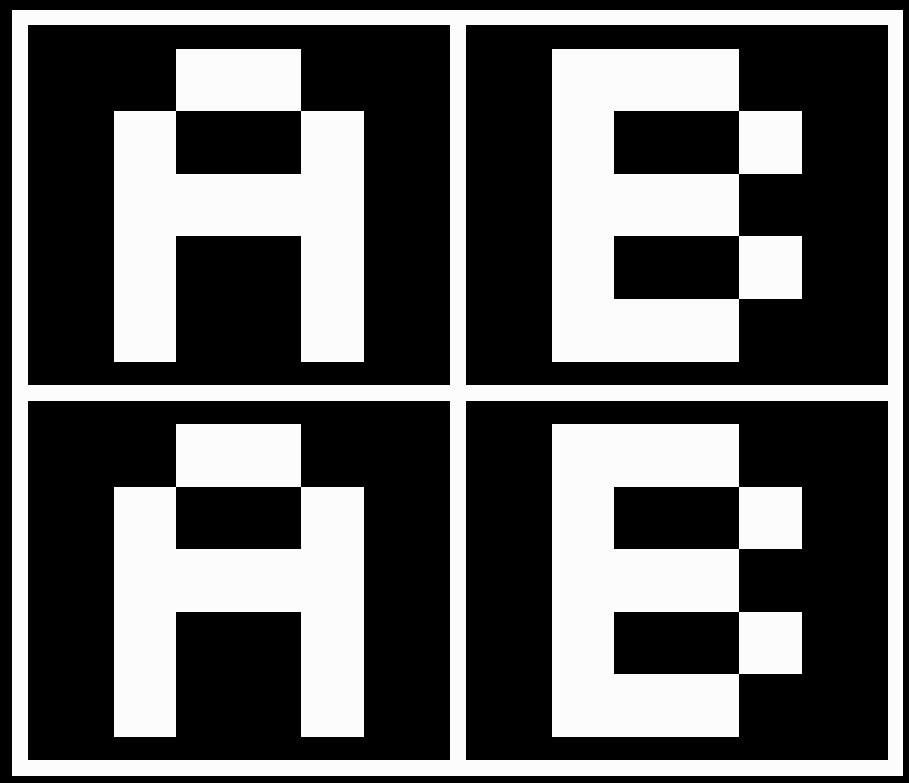
RESET BUTTON

-NAMETABLES-

- SET BACKGROUND TILES ON THE NAMETABLES
- BACKGROUND IS ACTUALLY 2 SCREENS WIDE & HIGH
- SCREEN (CAMERA) X & Y COORDINATES CAN BE INDEPENDENTLY SET
- NAMETABLES MIRRORED

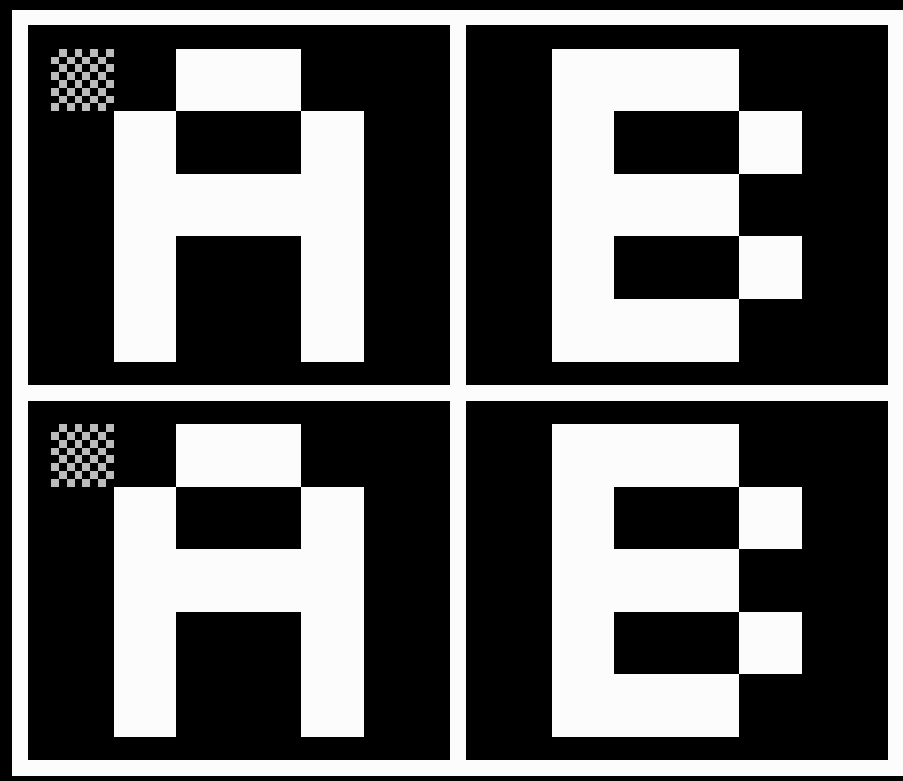

-NAMETABLES (2)-
PPU
$2000-
$23FF
PPU
$2400-
$27FF
PPU
$2800-
$2BFF
PPU
$2C00-
$2FFF
B - PREV A - NEXT

-VERTICAL MIRRORING-



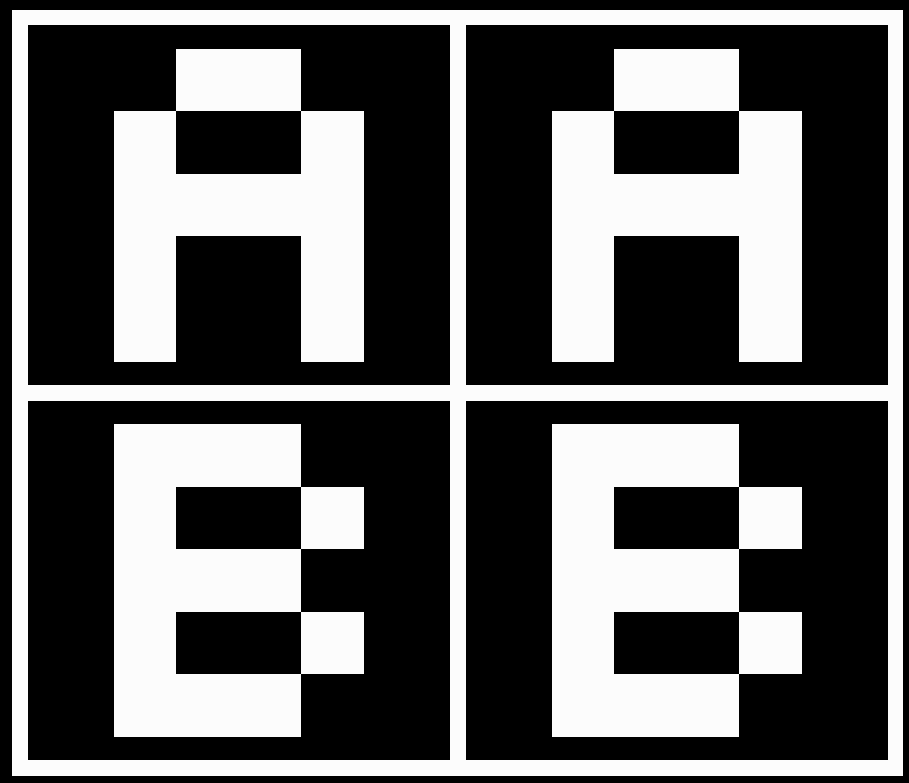
B - PREV A - NEXT

-VERTICAL MIRRORING-



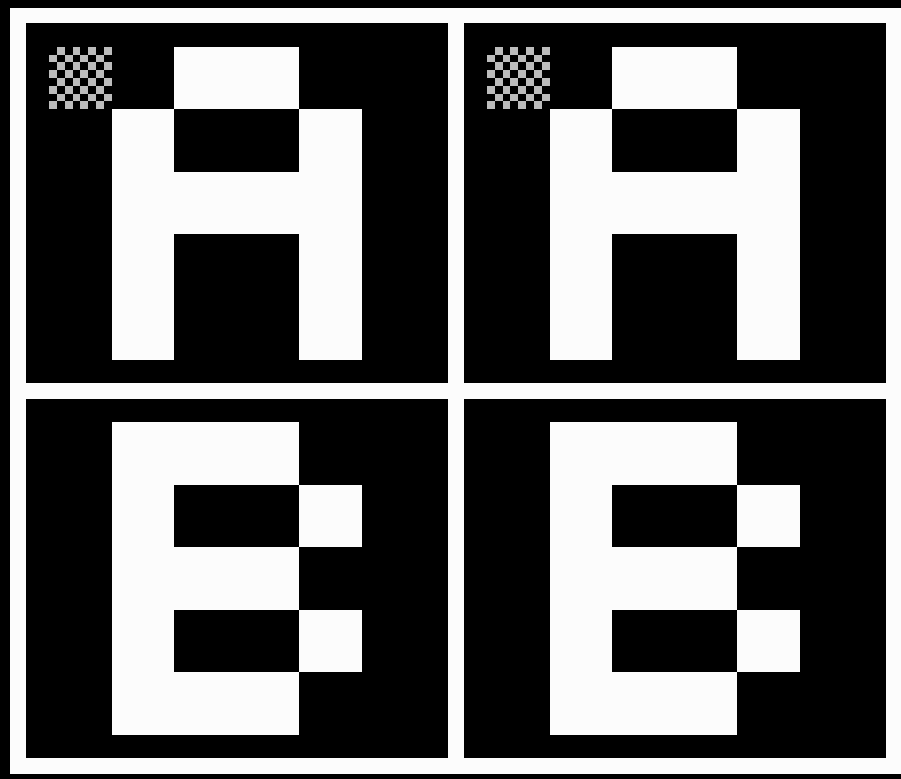
B - PREV A - NEXT

-HORIZONTAL MIRRORING-



B - PREV A - NEXT

-HORIZONTAL MIRRORING-



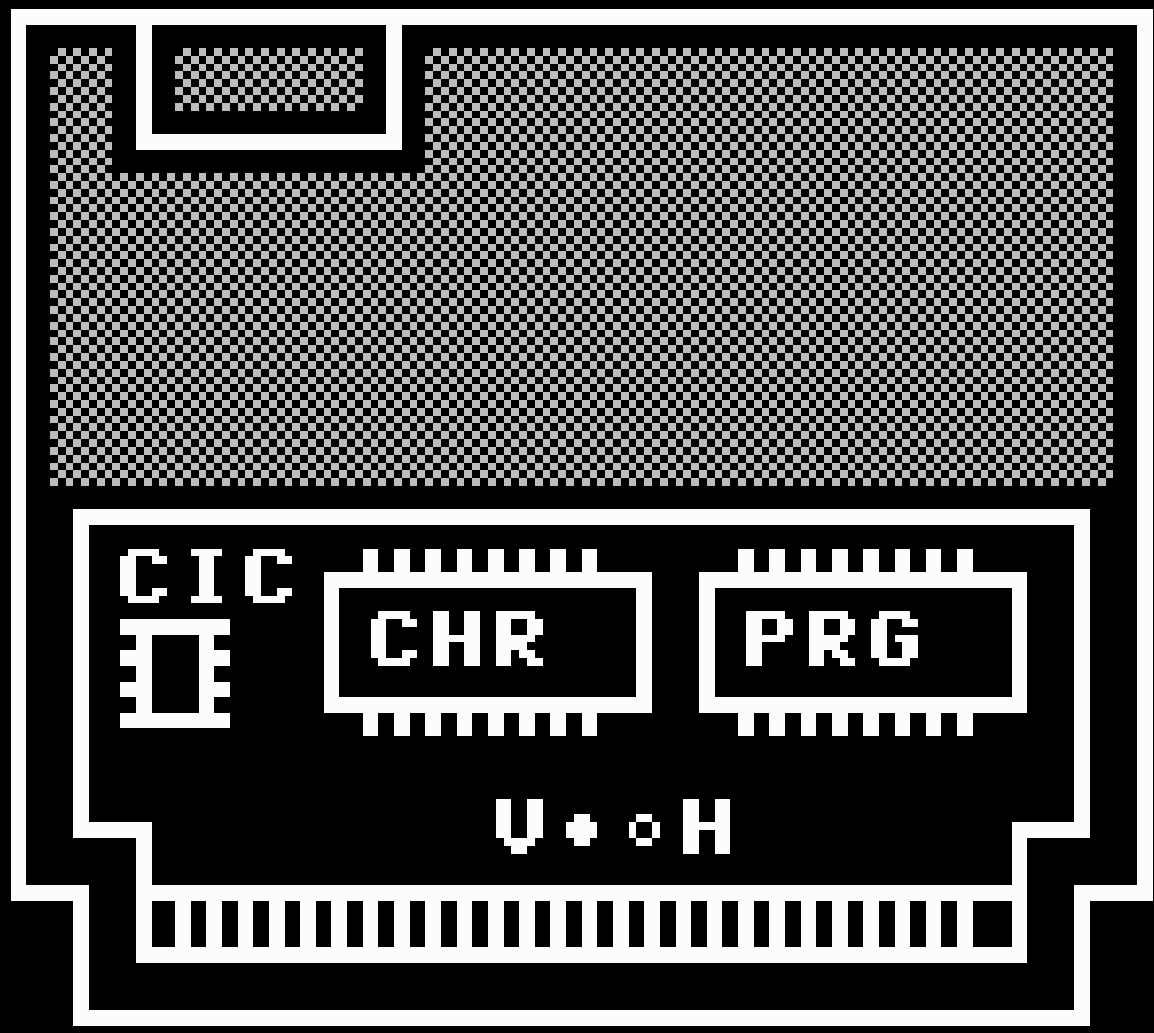
B - PREV A - NEXT

-MIRRORING-

- SET PPU $2000 TILE
- CHECK IF PPU $2400 TILE IS THE SAME TILE
- HORIZONTAL MIRRORING IF PPU $2000 AND $2400 ARE THE SAME
- OTHERWISE VERTICAL MIRRORING

B - PREV A - NEXT

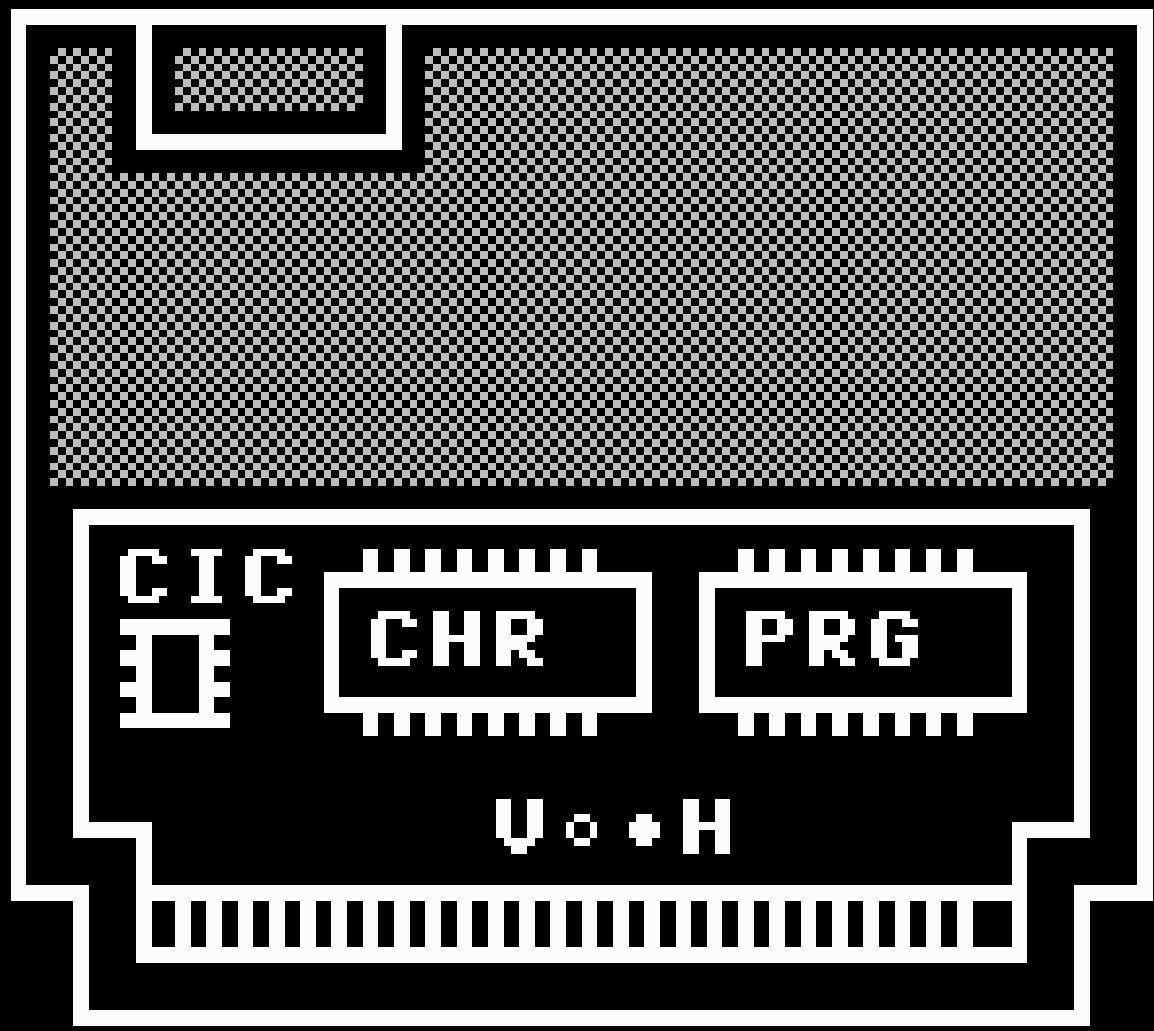
-MIRRORING (2)-



B - PREV A - NEXT

Vertical Mirroring (H solder pad)

-MIRRORING (2)-



B - PREV A - NEXT

-REGION DETECTION-

- NTSC - 60 FPS VIDEO
- PAL - 50 FPS VIDEO
  CPU SLOWER THAN NTSC
- DENDY - 50 FPS VIDEO
  CPU AS FAST AS NTSC
- CAN DETECT REGION BY
  COUNTING CPU CYCLES IN
  A SINGLE VIDEO FRAME

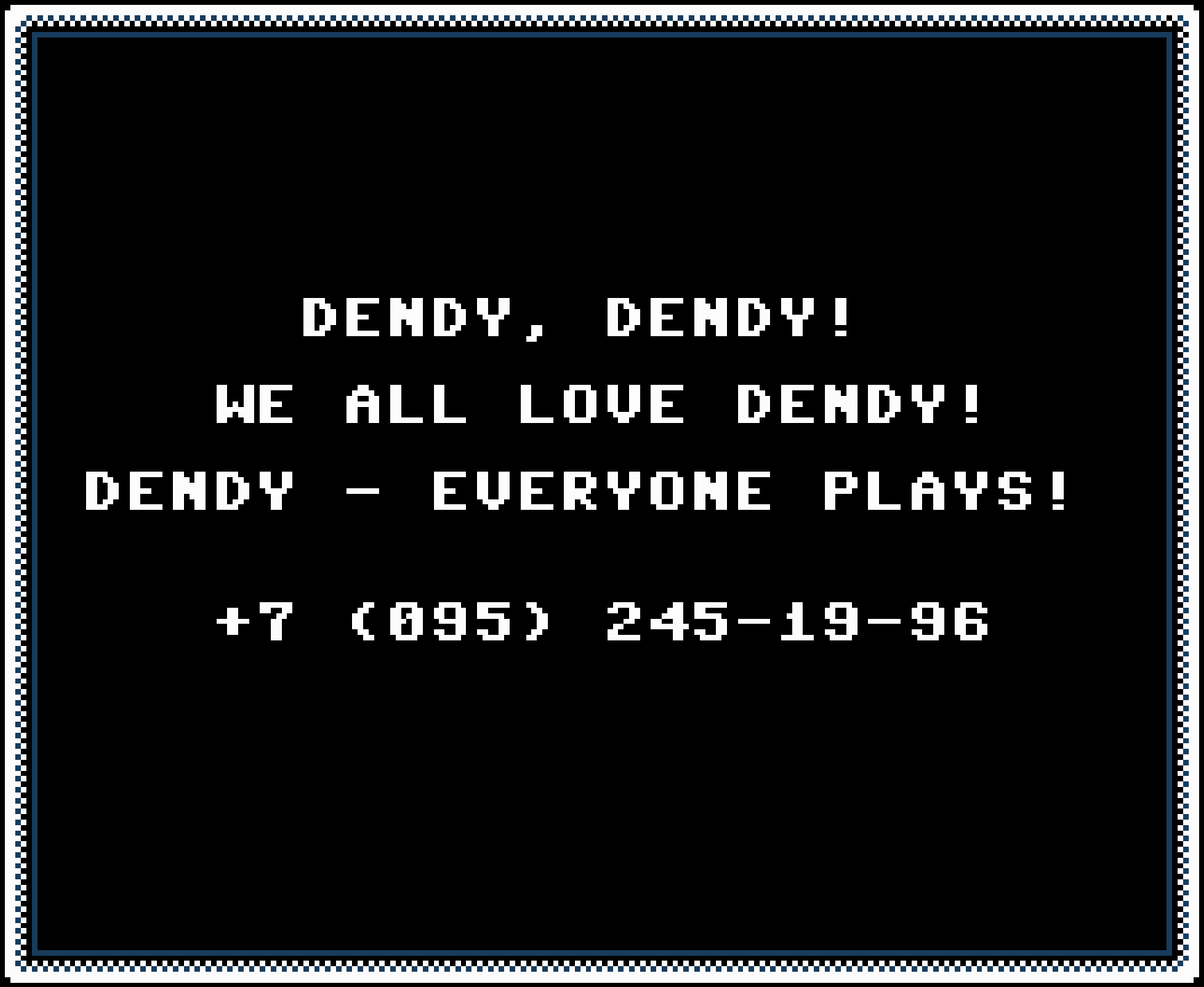
B - PREV A - NEXT

Start Screen on PAL Region NES

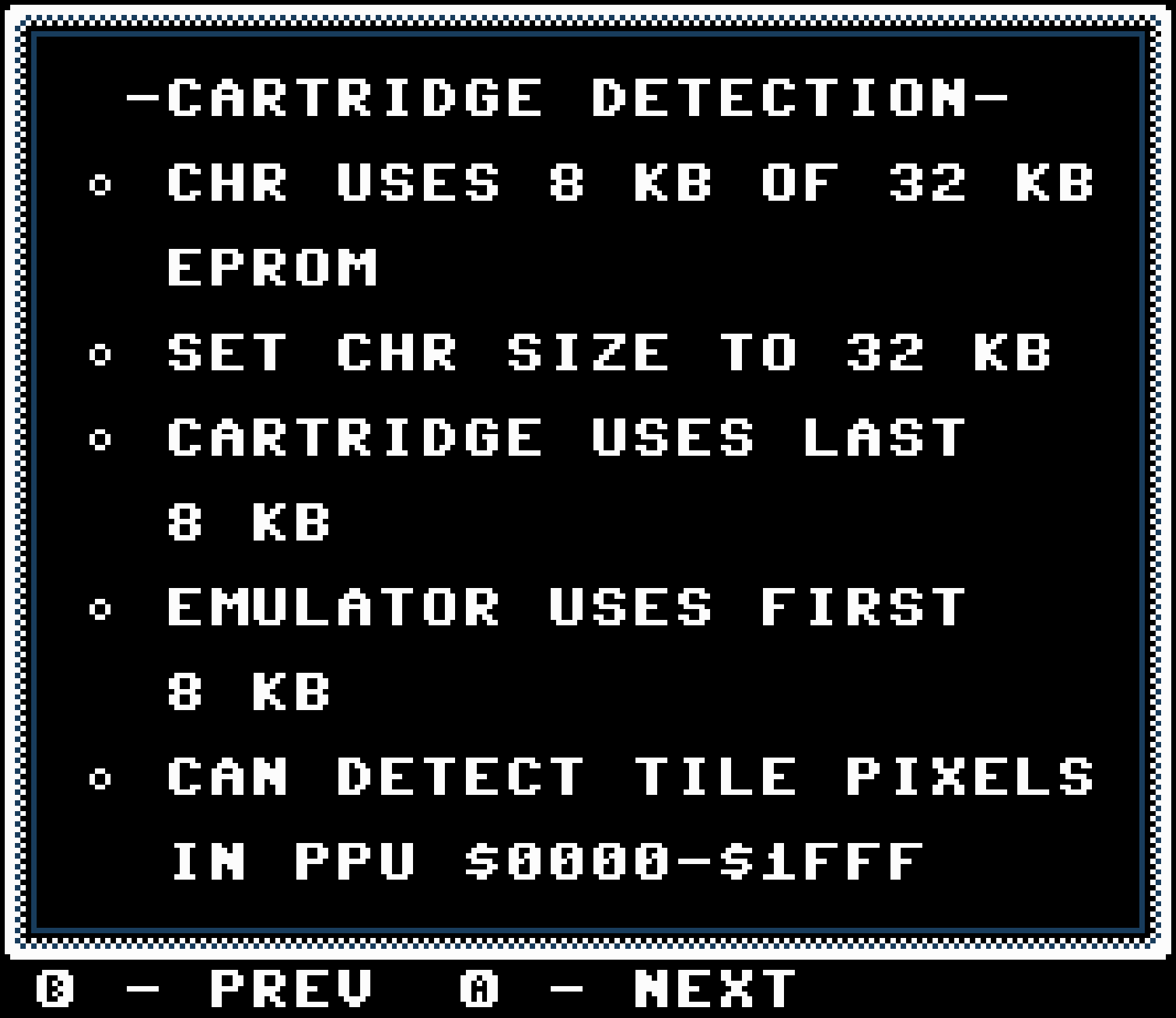
WE HAVE UPDATED OUR PRIVACY POLICY. YOUR TRUST IS IMPORTANT TO US.

A - CONTINUE

Start Screen on Dendy



A - CONTINUE


-CARTRIDGE DETECTION-
CHR USES 8 KB OF 32 KB EPROM
SET CHR SIZE TO 32 KB
CARTRIDGE USES LAST 8 KB
EMULATOR USES FIRST 8 KB
CAN DETECT TILE PIXELS IN PPU $0000-$1FFF
B - PREV A - NEXT

-CART DETECTION (2)-

B - PREV A - NEXT

-CART DETECTION (2)-

B - PREV A - NEXT

hopexii.nes running on emulator

NES ROM FILE

I Dream of Game Genies and ZIP Files

Hacking the NES

20 JULY 2018

PRESENTED BY VI GREY

START PRESENTATION

SPECIAL THANKS

VIGREY.COM - TWITTER.COM/@VIGREYTECH

#HOPECONF

#HOPEXII

hopexii.nes running on emulator

-ACT 2-

POLYGLOT FILES

B - PREV A - NEXT

-POLYGLOT FILES-

- FILES THAT EXIST AS 2 OR MORE DISTINCT FILE TYPES SIMULTANEOUSLY
- SOME FILE TYPES HAVE DATA THAT MUST START AT BEGINNING OF FILE OR END AT END OF FILE AND SOME DO NOT CARE

-POLYGLOT FILES (2)-

- STRICT START:
  NES, JPEG, BITMAP, MP3
- FLEXIBLE START/END:
  ZIP, 7Z, RAR

B - PREV A - NEXT

-POLYGLOT FILES (3)-

- THIS NES ROM DATA IS ALWAYS 65552 BYTES
- UNUSED PRG AND CHR DATA IS IGNORED
- PLACES WITH UNUSED DATA ARE A GREAT PLACE TO INSERT OTHER FILE DATA

B - PREV A - NEXT

-ZIP-

- NO STRICT BEGINNING OR END FOR FILE DATA
- "HEADER" OR END OF CENTRAL DIR. RECORD IS AT END OF FILE DATA
- OFFSETS IN ZIP FILE DATA CAN BE UPDATED

-7Z & RAR-

- NO STRICT BEGINNING OR END FOR FILE DATA
- DO NOT NEED TO UPDATE ANY OFFSETS

-ZIP/7Z/RAR-

- EXTRACTORS WILL OFTEN ASSUME FILE IS FIRST TYPE OF FILE IN DATA (ZIP IN THIS CASE)
- "7Z -T7Z X" COMMAND CAN EXTRACT 7Z FILE
- "UNRAR X" COMMAND CAN EXTRACT RAR FILE

-HTML-

- VERY FLEXIBLE FORMAT
- MISSING TAGS OFTEN ASSUMED BY BROWSER
- EXTRA DATA RISKS BEING INTERPRETED AS TEXT

-HTML (2)-

EXTRA TEXT

<DIV>

  HELLO WORLD

</DIV>

-HTML (3)-

```
<!DOCTYPE HTML>
<HTML>
   <BODY>
      EXTRA TEXT
      <DIV>
         HELLO WORLD
      </DIV>
   <BODY>
</HTML>
```

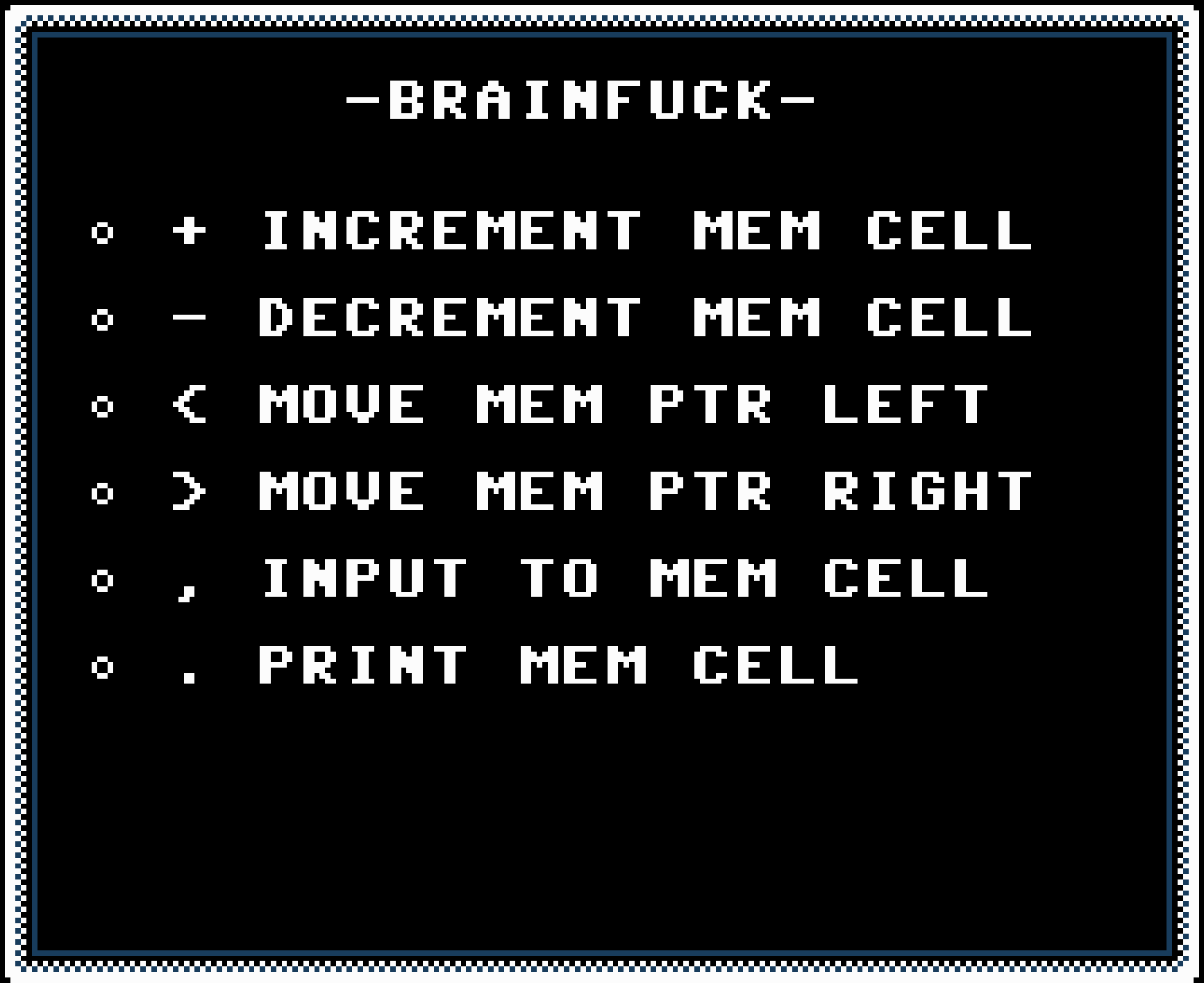
B - PREV A - NEXT

-HTML (4)-

- SET FONT-SIZE OF BODY TO 0 AND VISIBILITY TO HIDDEN
- SET FONT-SIZE OF INNER DIV TO 16PX AND VISIBILITY TO VISIBLE
- COMMENT EVERYTHING ELSE WITH <!--

-HTML (5)-

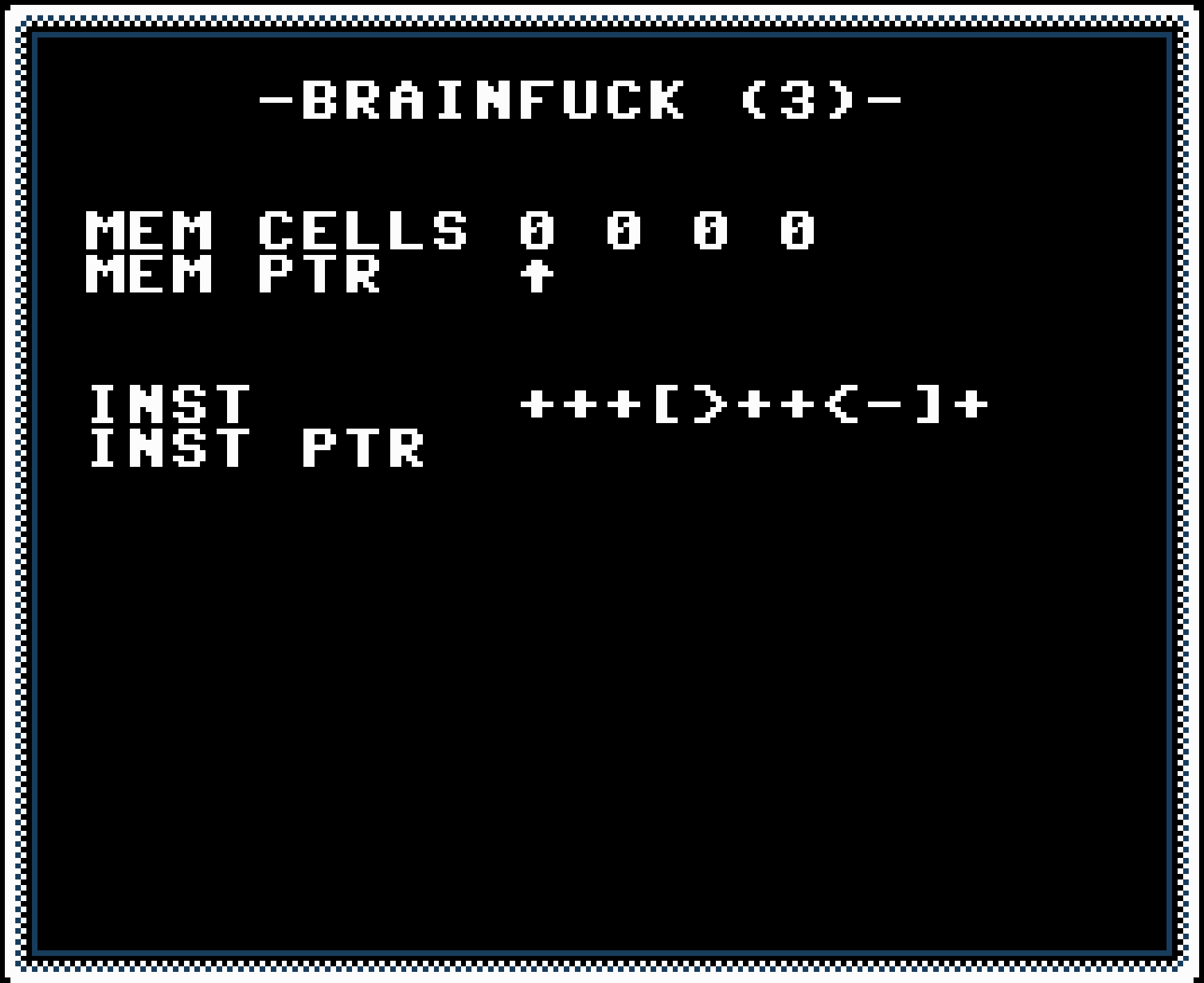
```
BODY {
   FONT-SIZE: 0;
   VISIBILITY: HIDDEN;
}
DIV {
   FONT-SIZE: 16PX;
   VISIBILITY: VISIBLE;
}
```

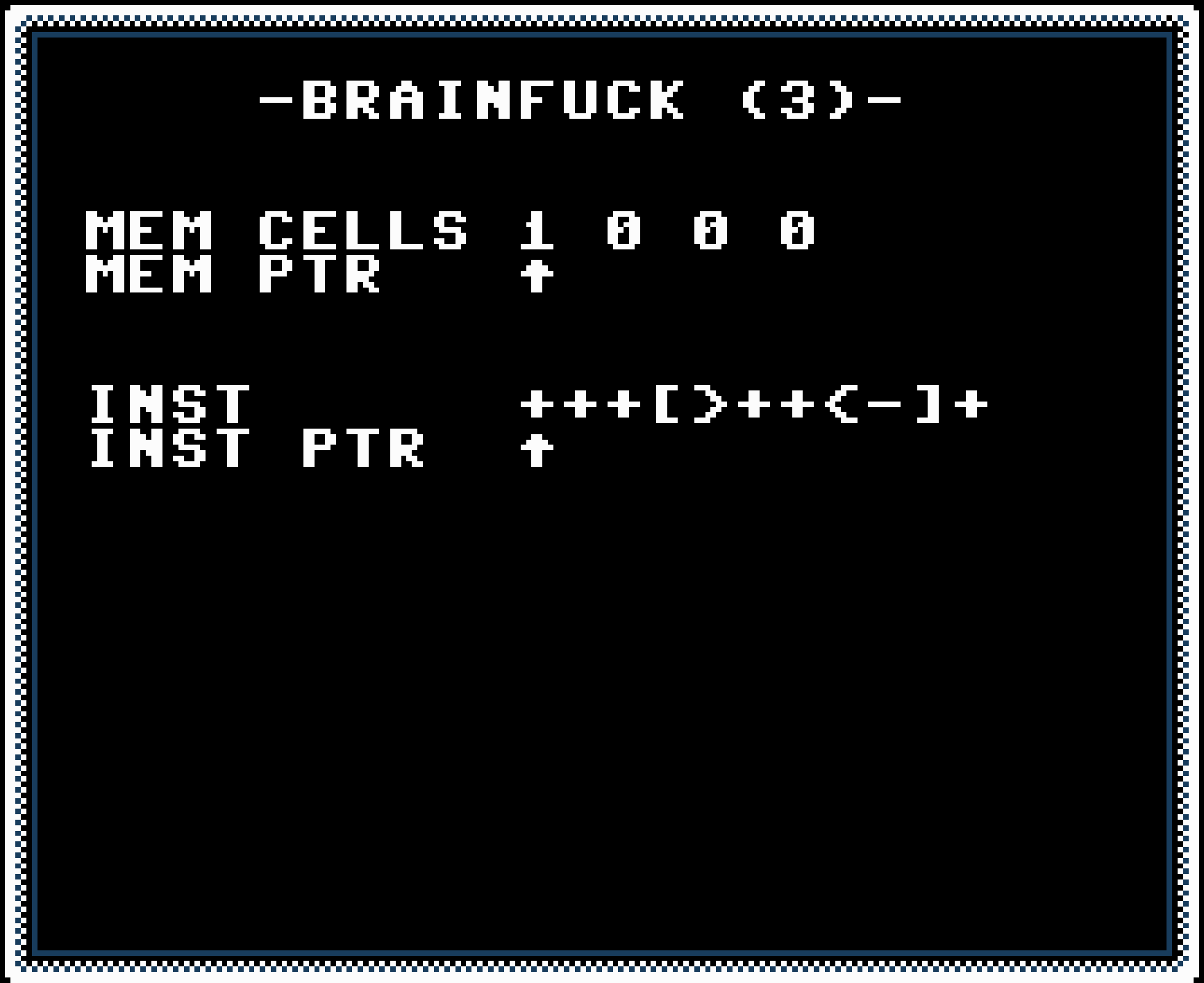

-BRAINFUCK-
+ INCREMENT MEM CELL
- DECREMENT MEM CELL
< MOVE MEM PTR LEFT
> MOVE MEM PTR RIGHT
, INPUT TO MEM CELL
. PRINT MEM CELL

B - PREV A - NEXT

-BRAINFUCK (2)-

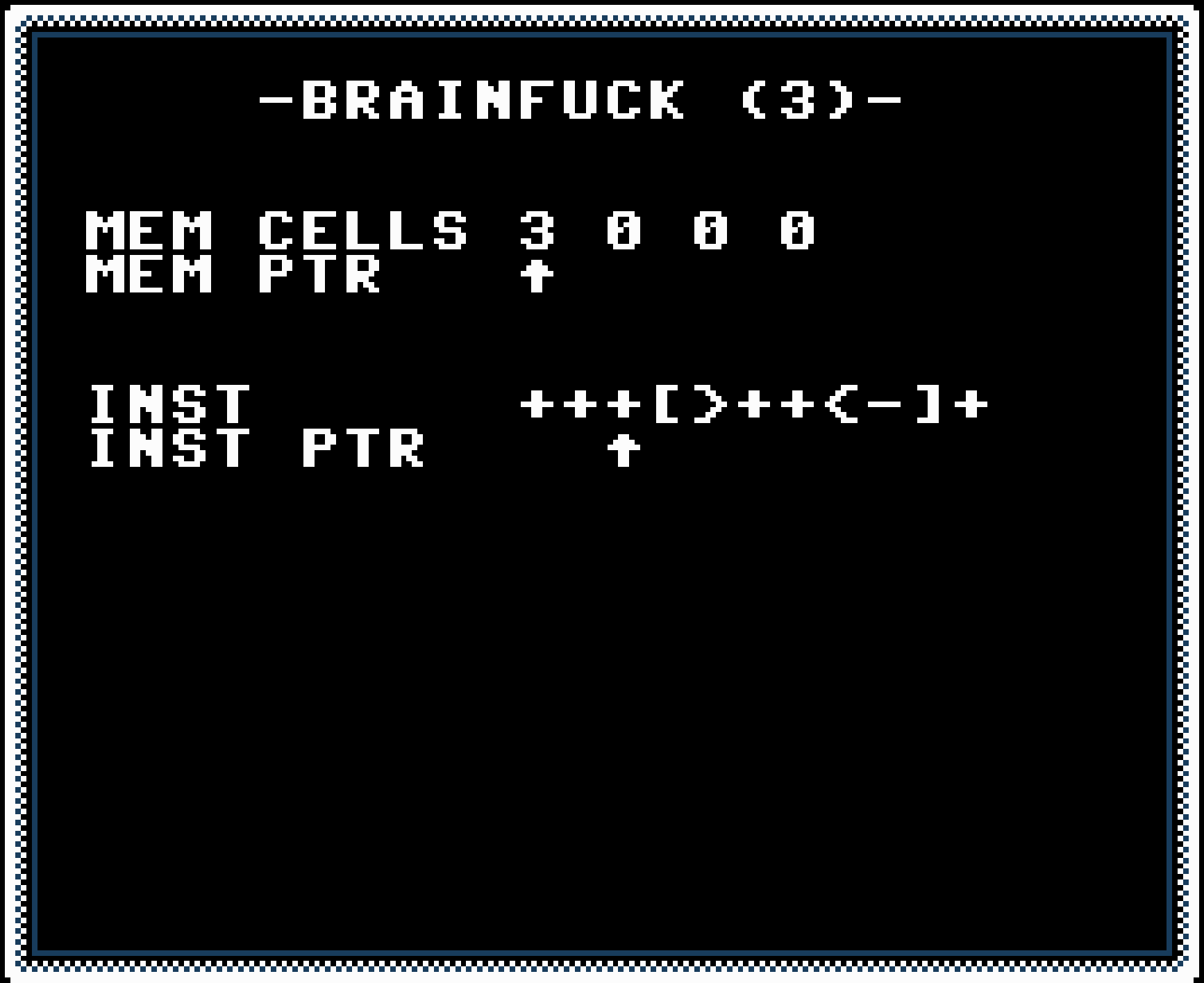
- [IF MEM CELL IS 0, MOVE INST PTR RIGHT PAST MATCHING]
-] MOVE INST PTR LEFT TO MATCHING [


-BRAINFUCK (3)-
MEM CELLS 0 0 0 0
MEM PTR ↑
INST +++[>++<-]+
INST PTR
B - PREV A - NEXT

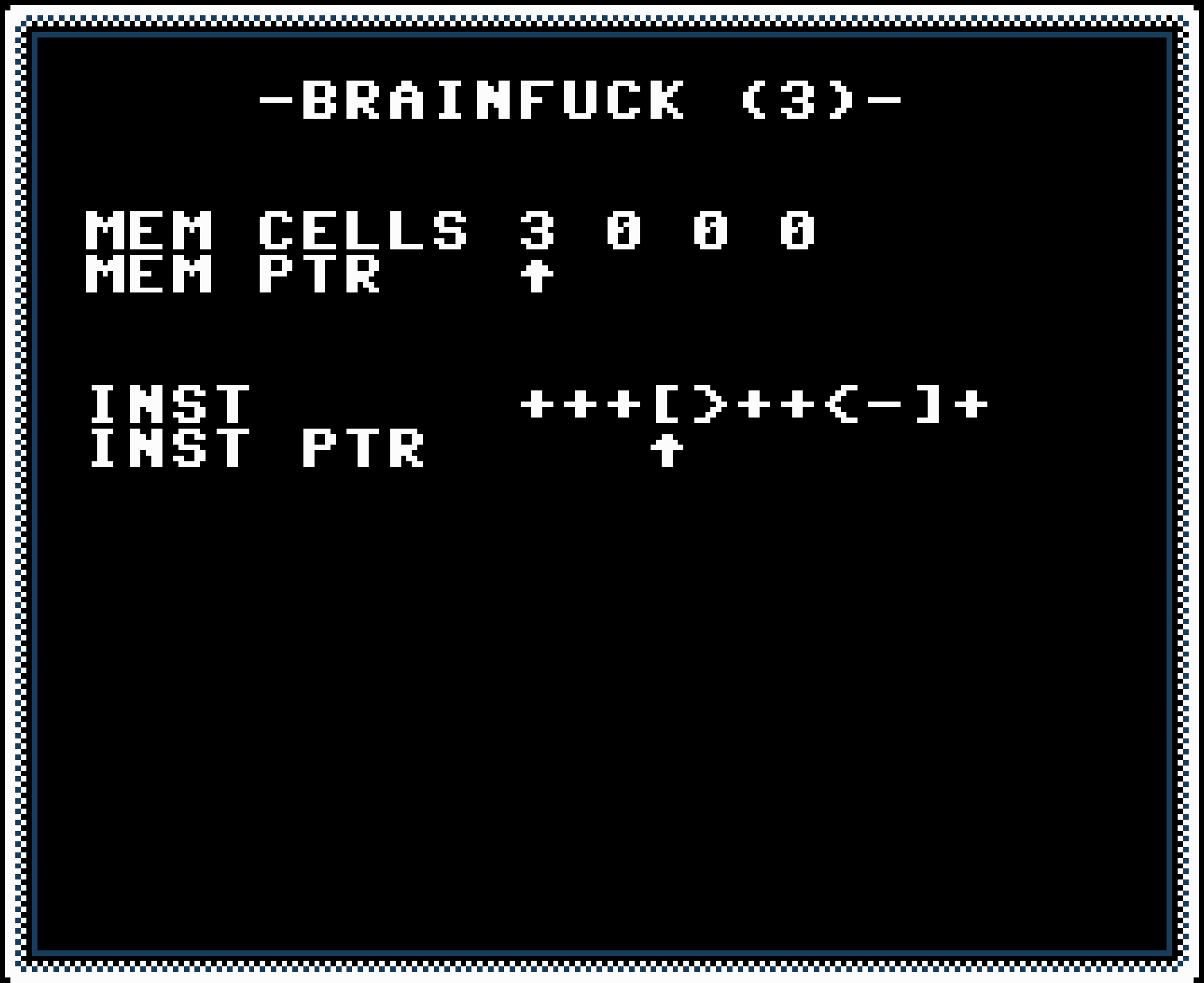


B - PREV A - NEXT

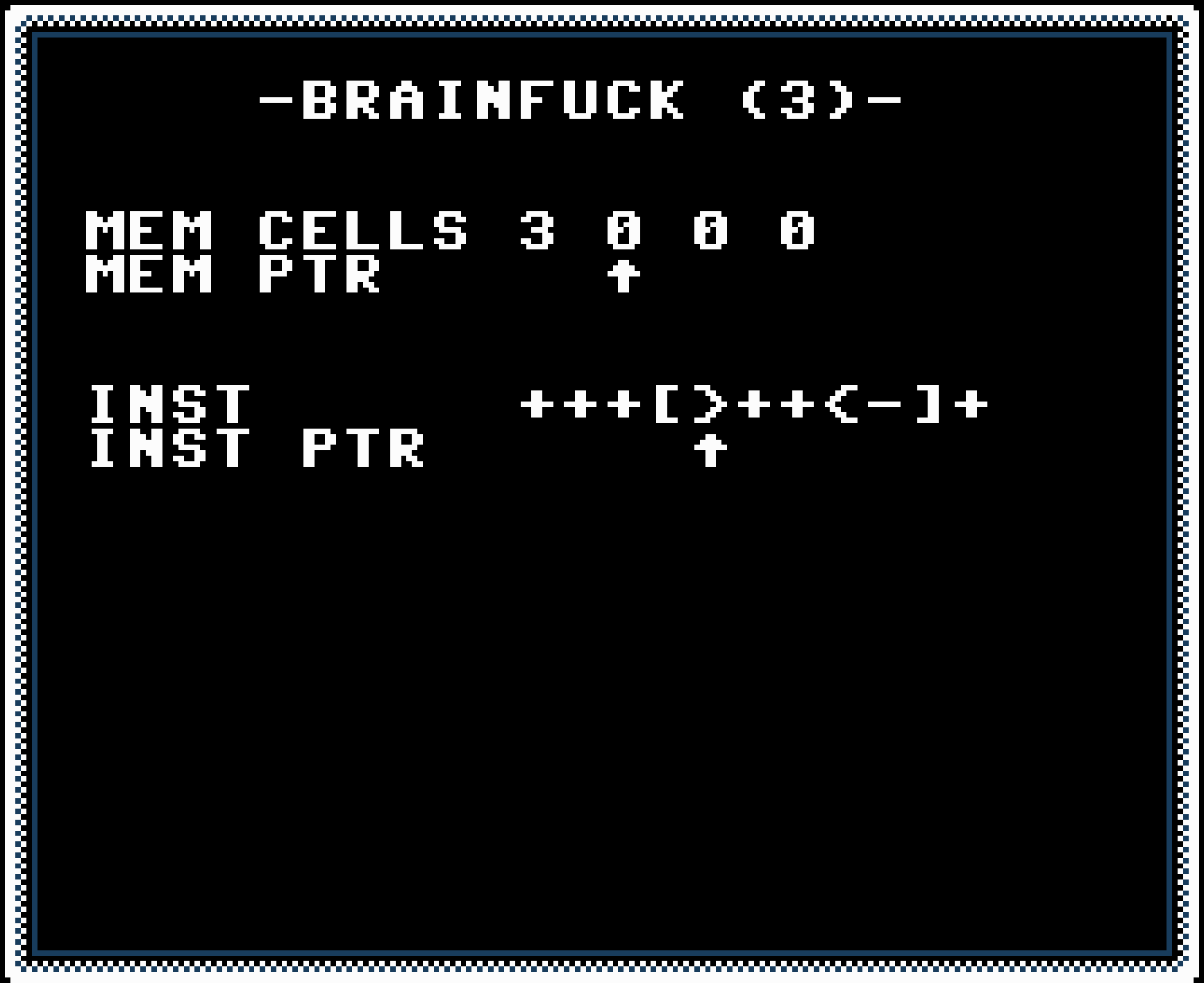
B - PREV A - NEXT



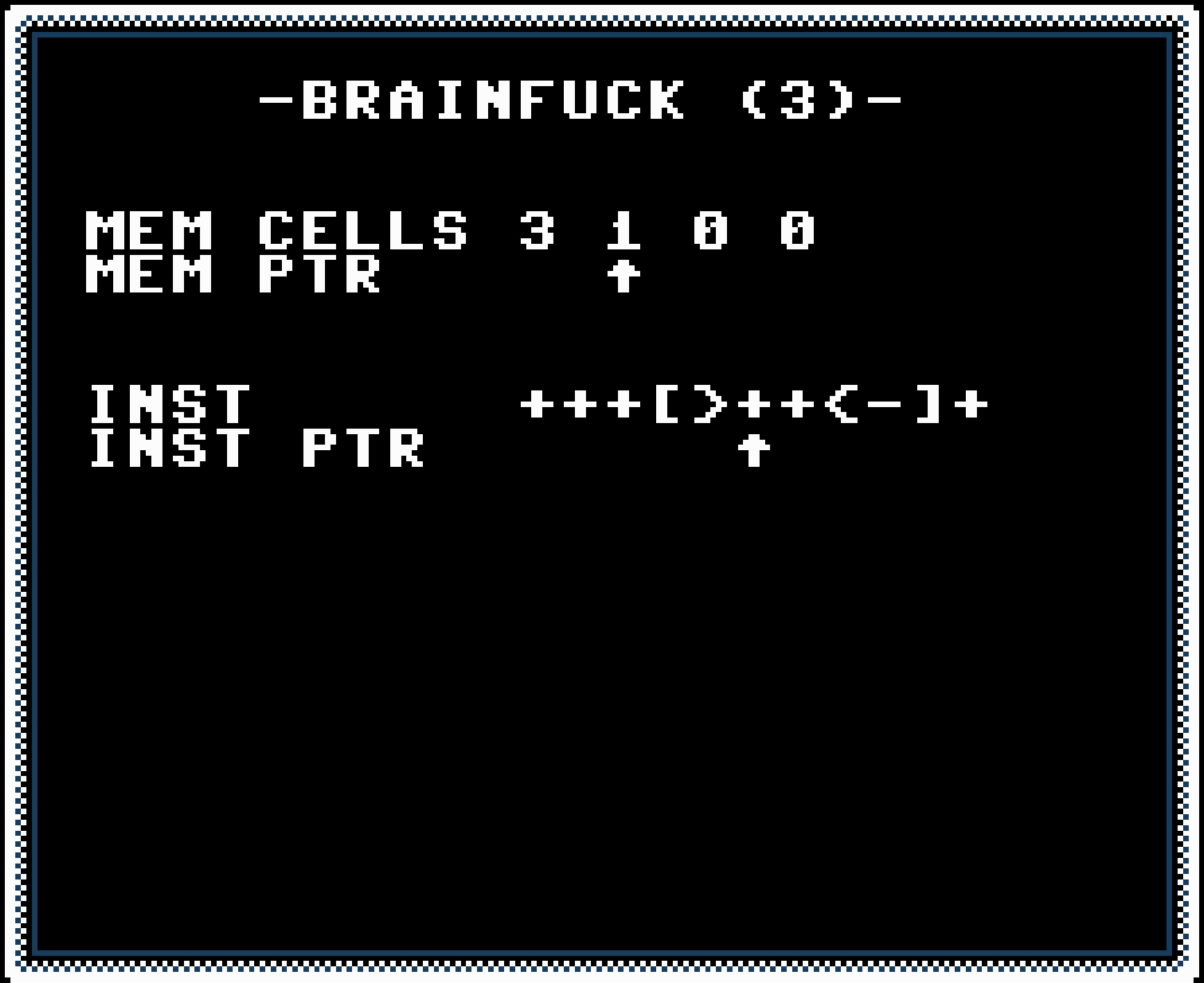
B - PREV A - NEXT



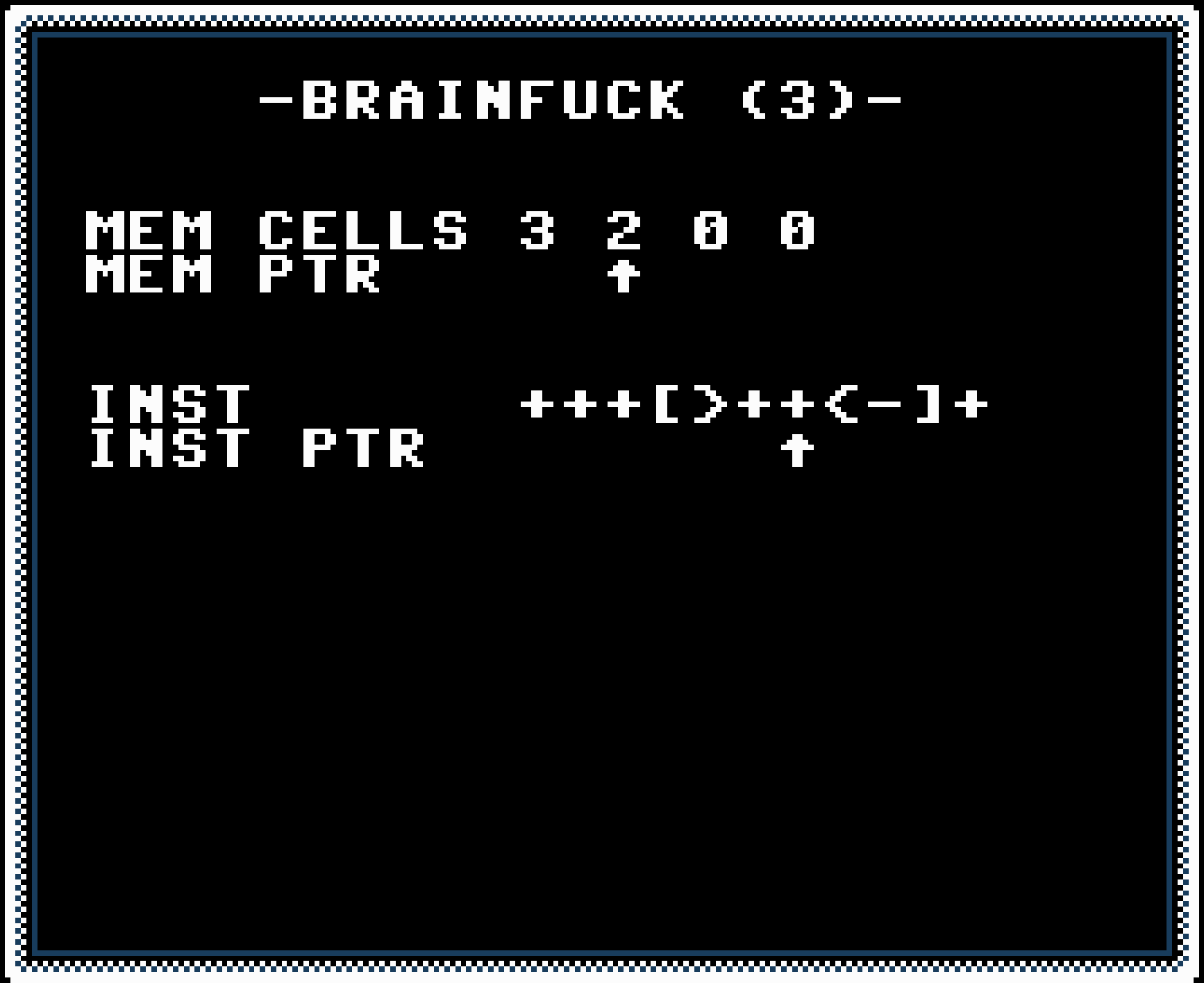
B - PREV A - NEXT

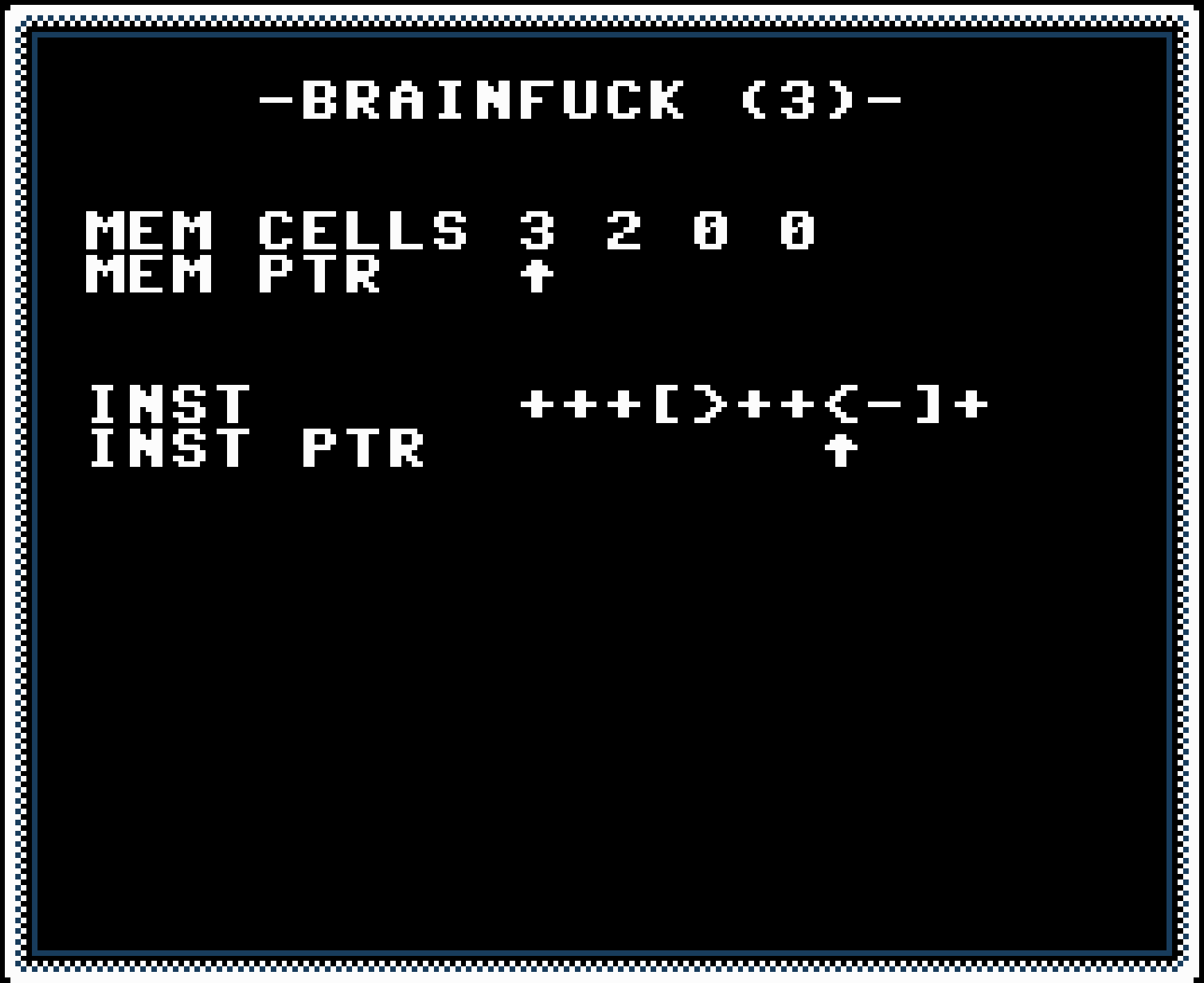


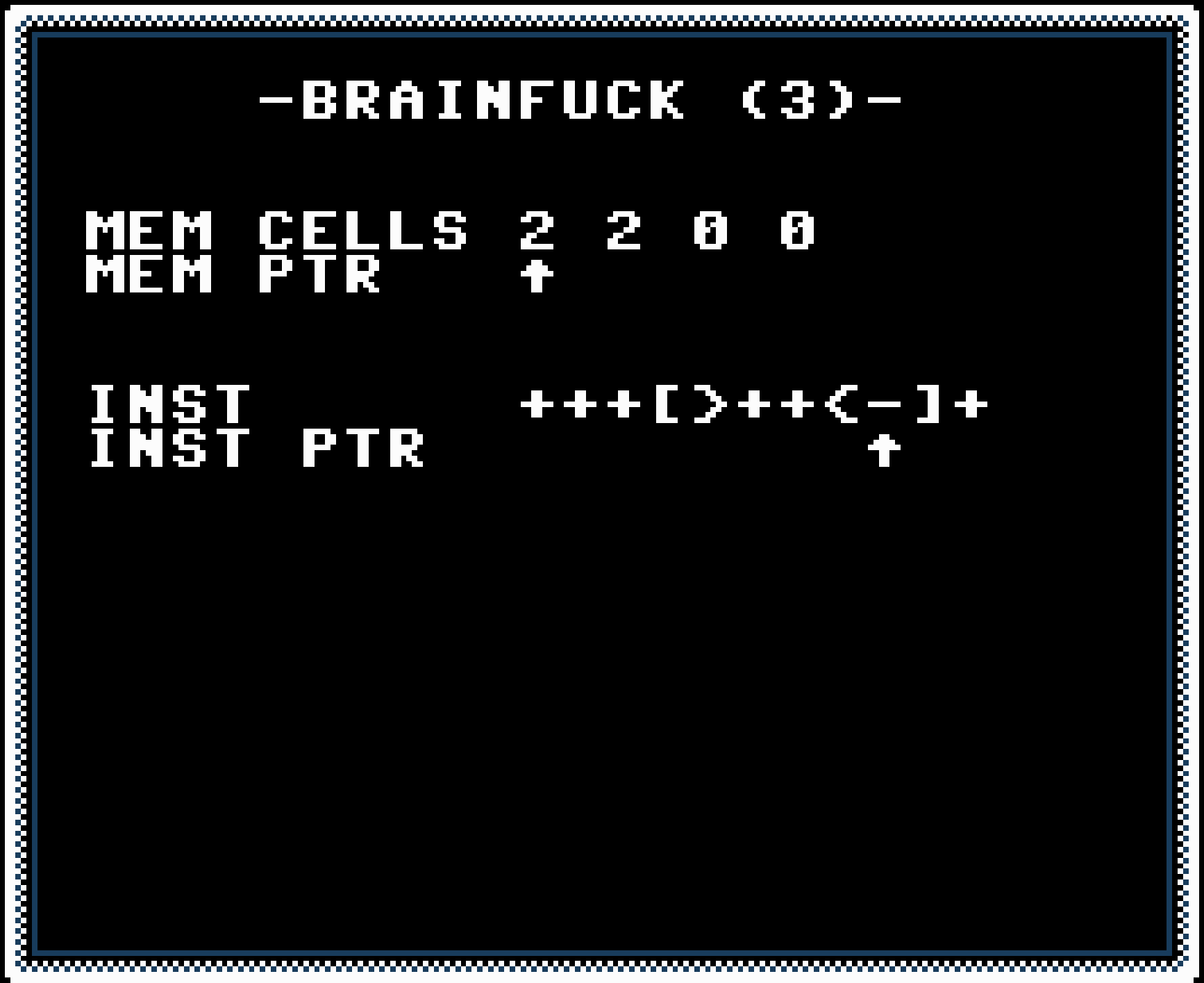
B - PREV A - NEXT



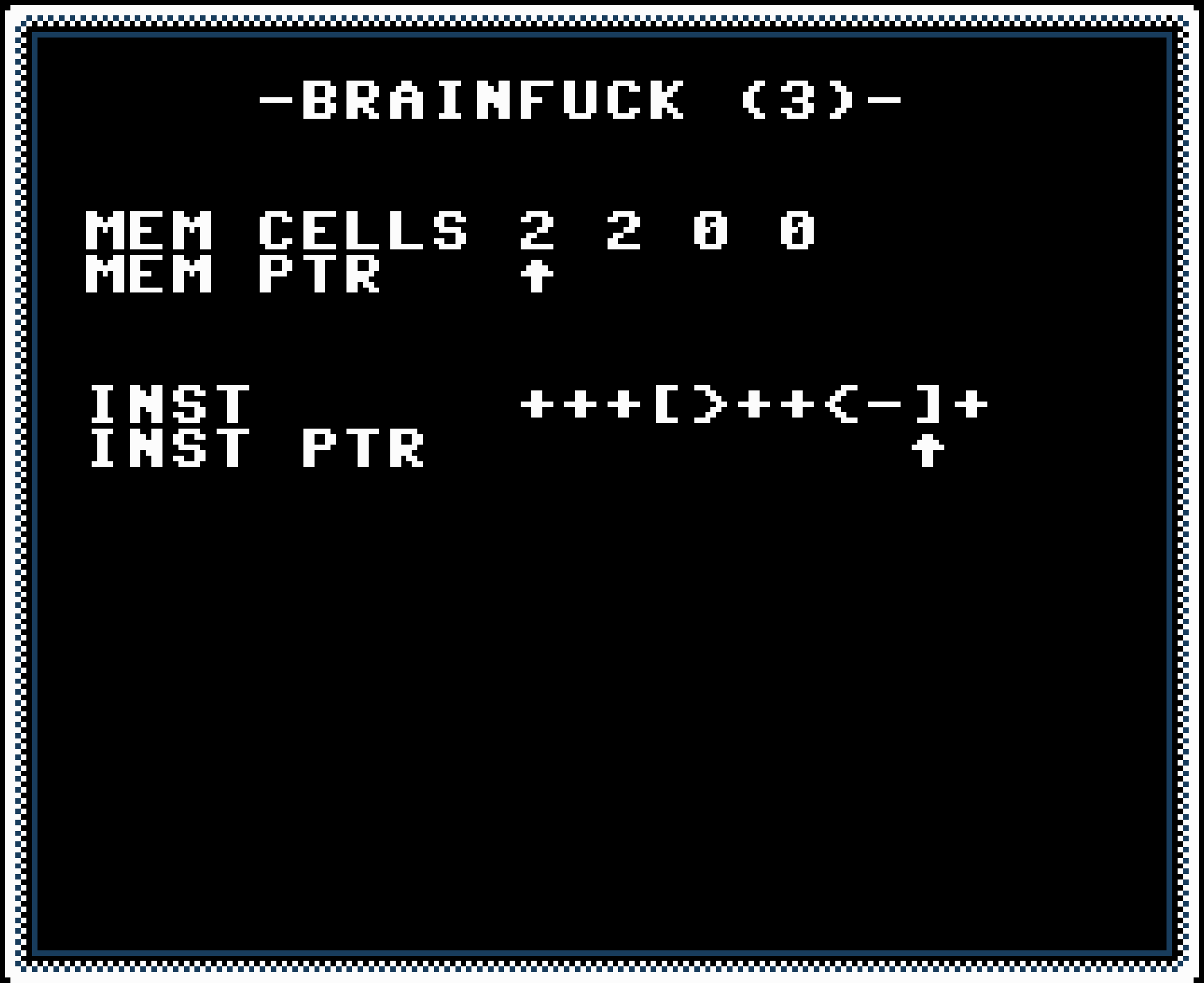
B - PREV A - NEXT


-BRAINFUCK (3)-
MEM CELLS 3 2 0 0
MEM PTR
INST +++[>++<-]+
INST PTR
0 - PREV 0 - NEXT

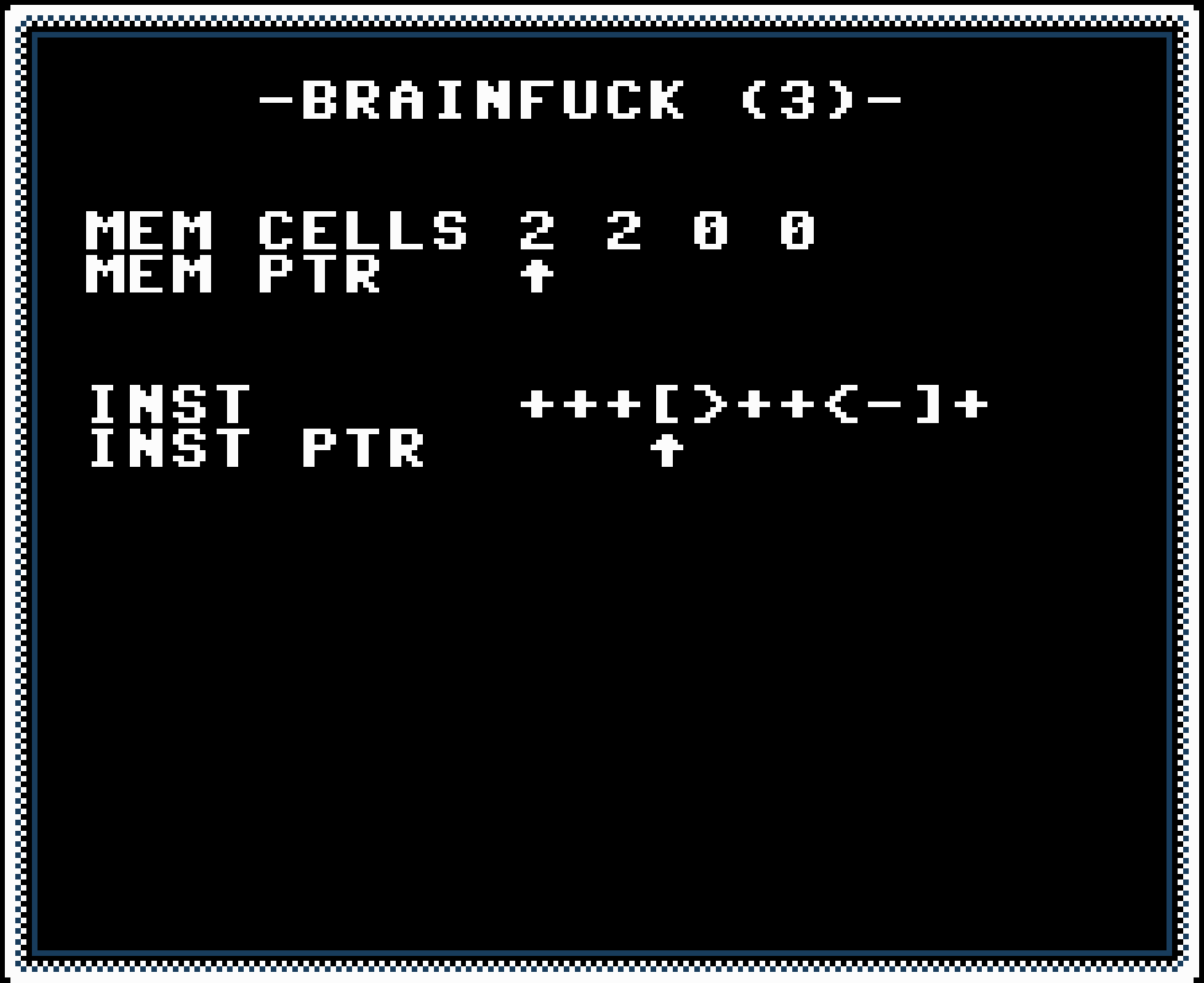

-BRAINFUCK (3)-
MEM CELLS 3 2 0 0
MEM PTR
INST +++[>++<-]+
INST PTR
B - PREV A - NEXT



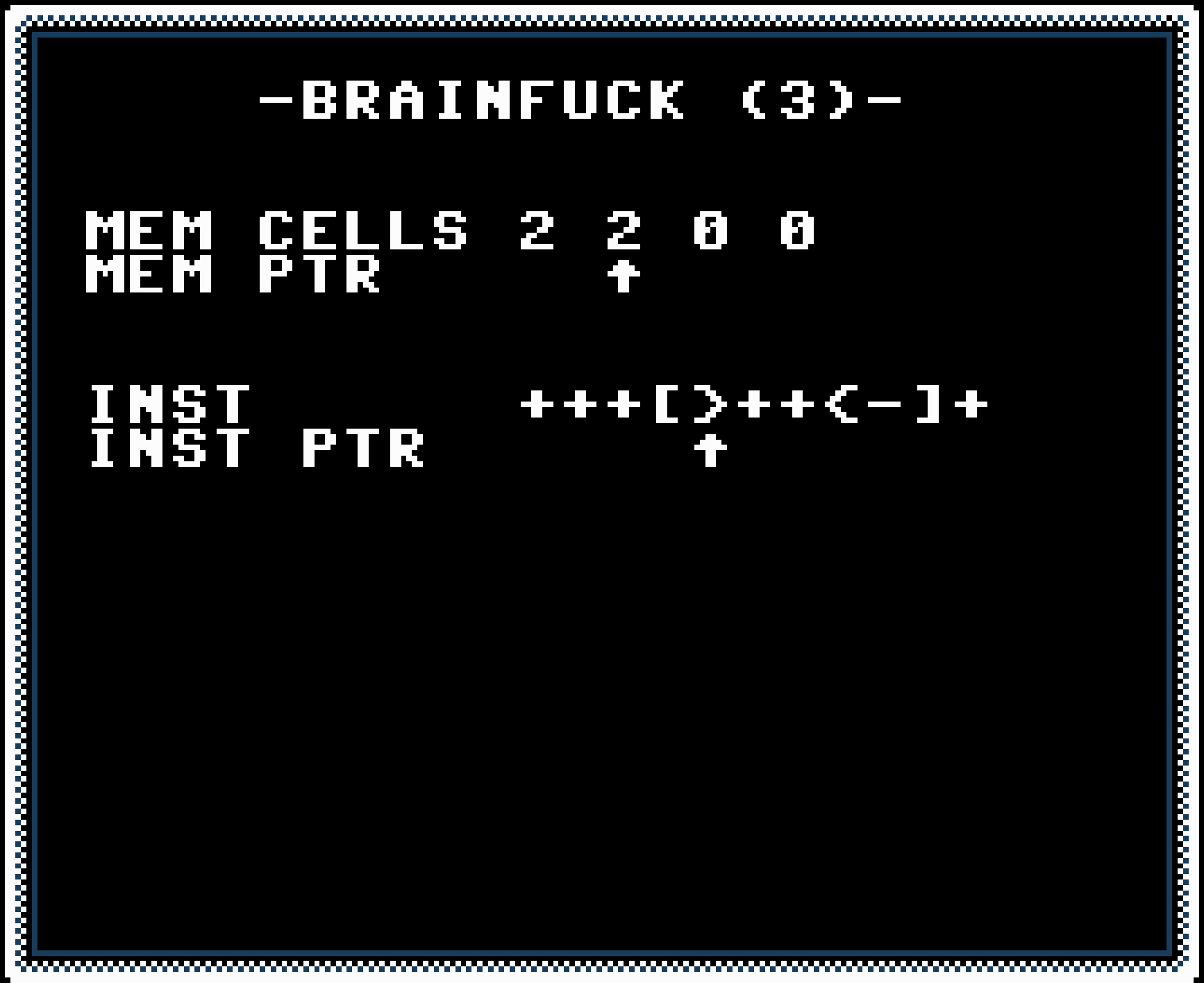
B - PREV A - NEXT

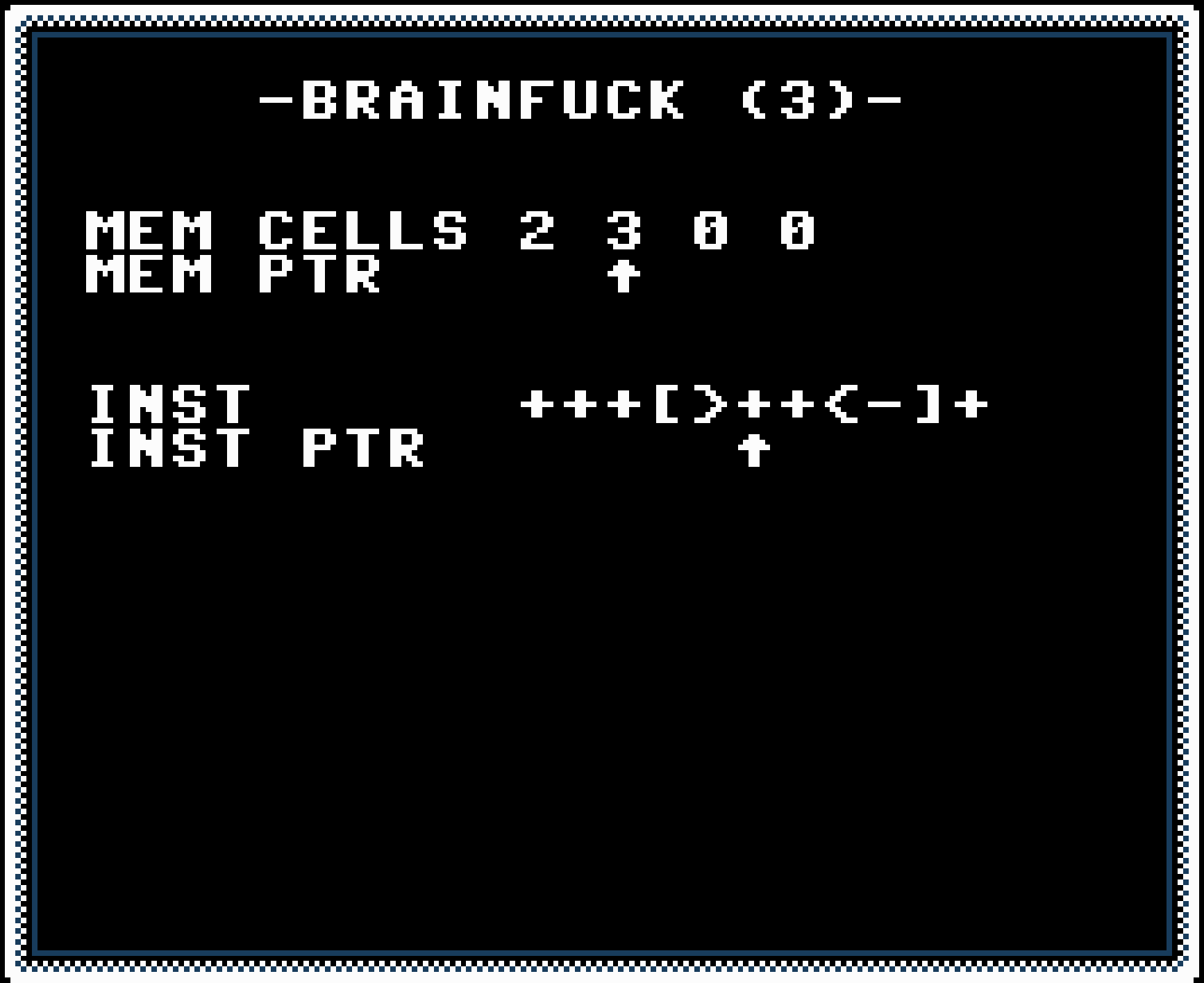


B - PREV A - NEXT

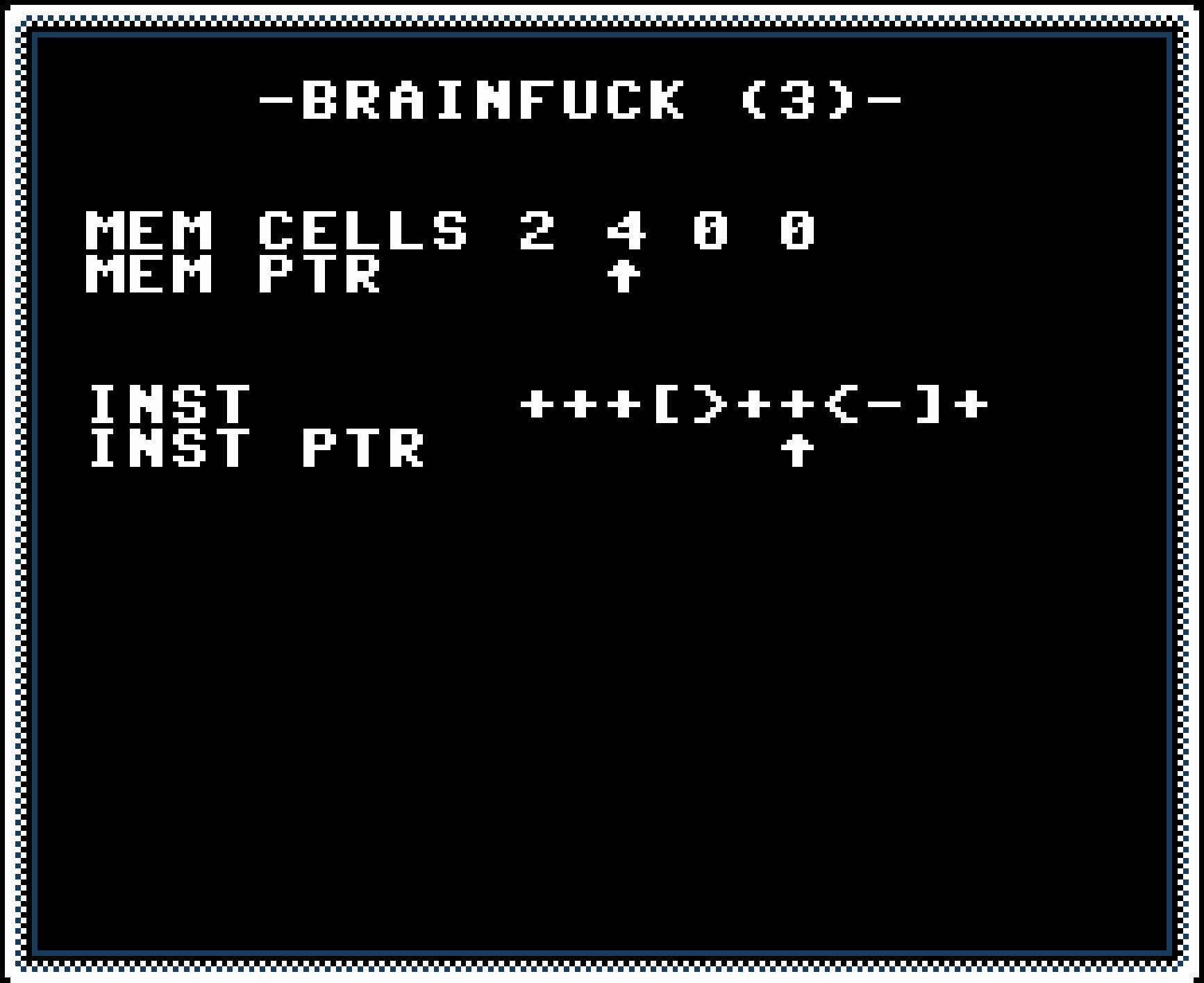


B - PREV A - NEXT

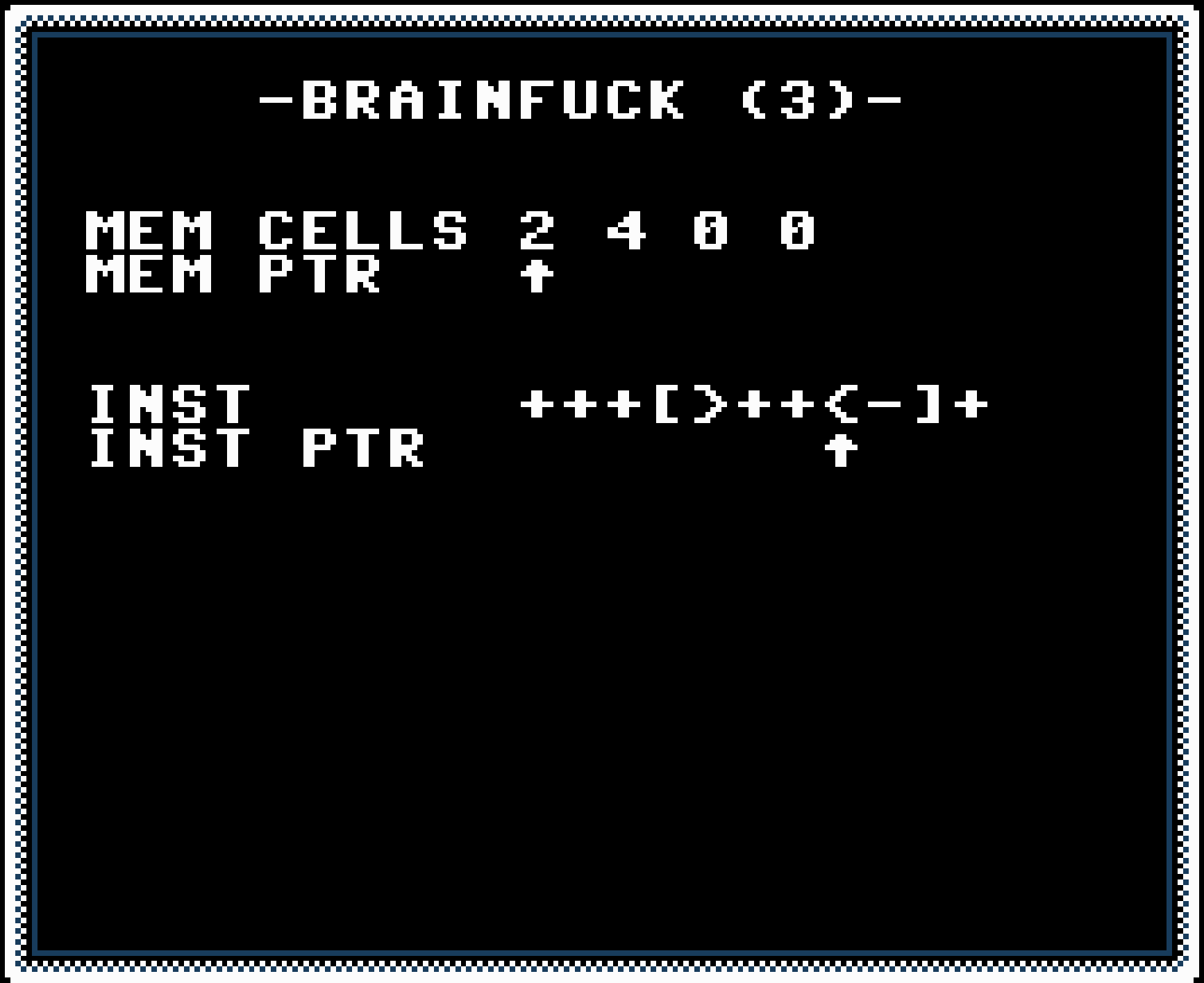

-BRAINFUCK (3)-
MEM CELLS 2 2 0 0
MEM PTR
INST +++[>++<-]+
INST PTR
0 - PREV 0 - NEXT



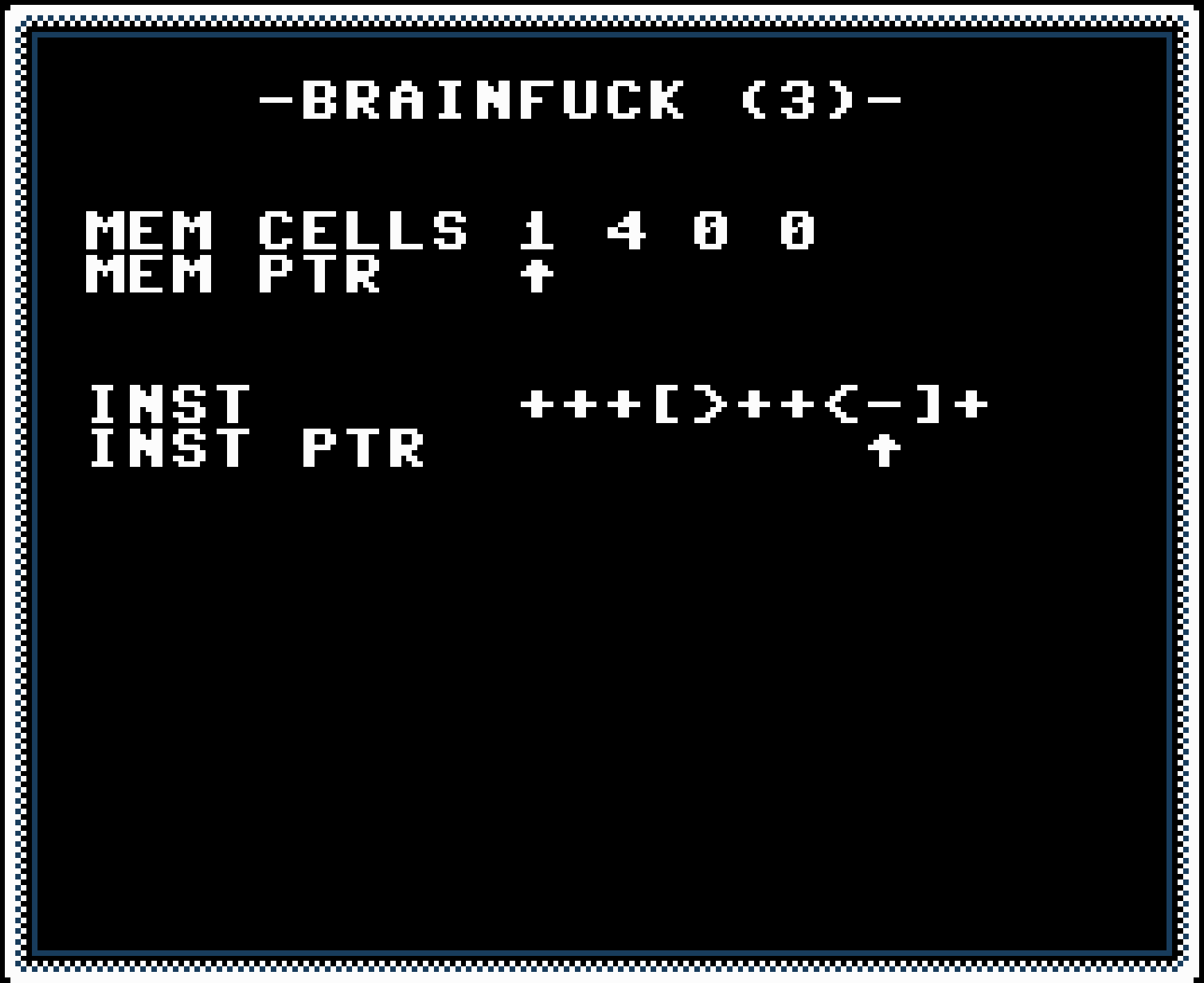
B - PREV A - NEXT



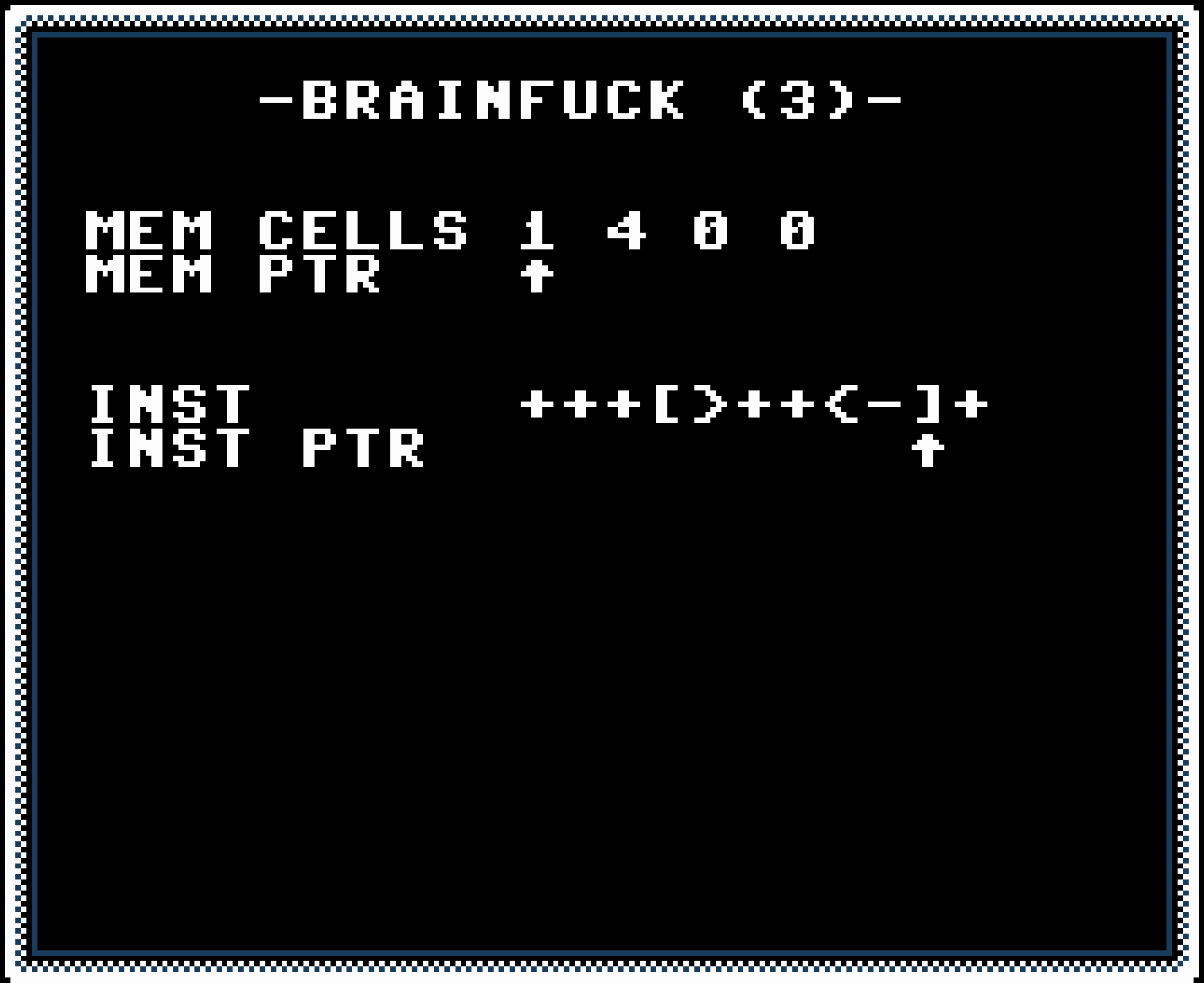
B - PREV A - NEXT



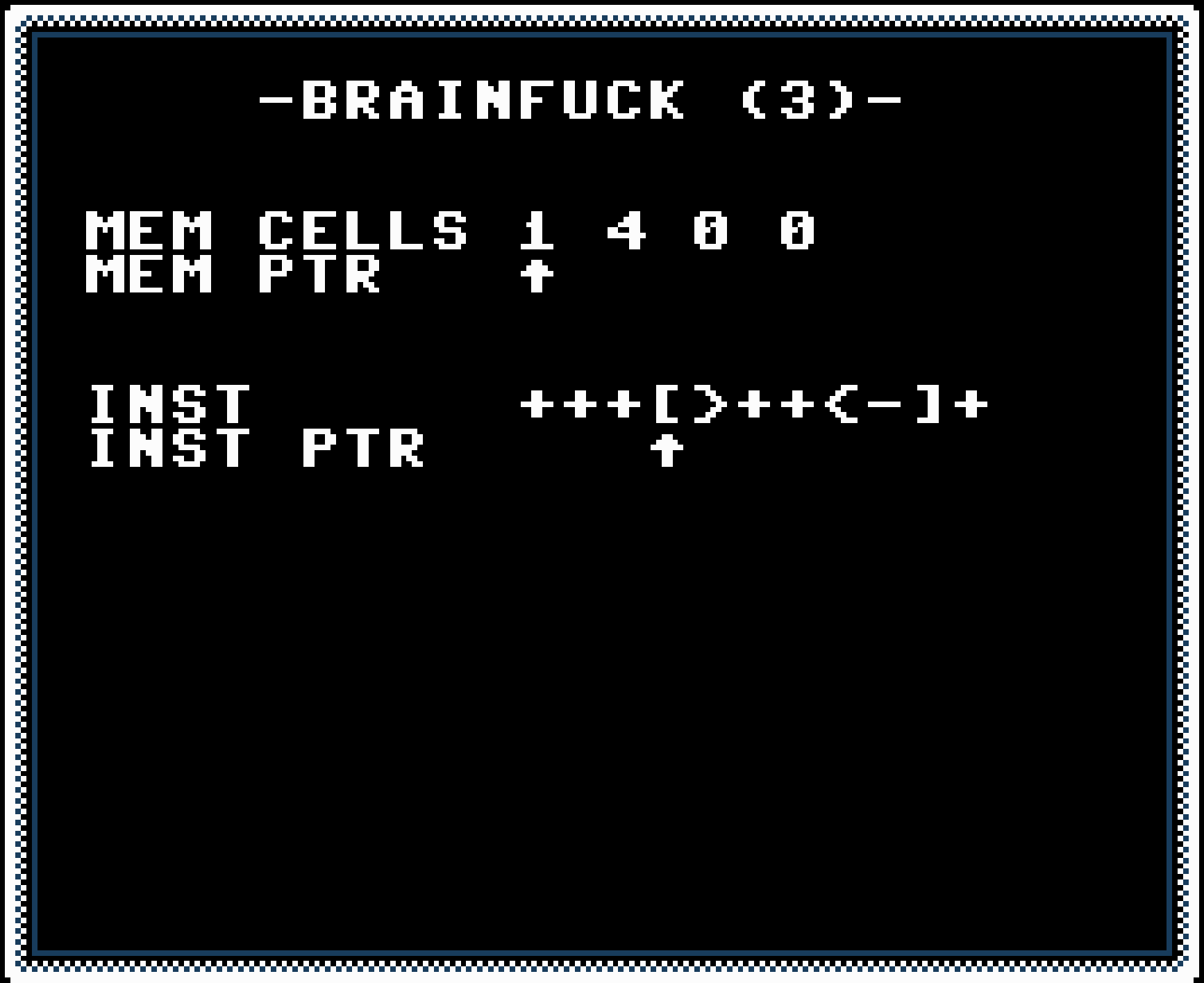
B - PREV A - NEXT



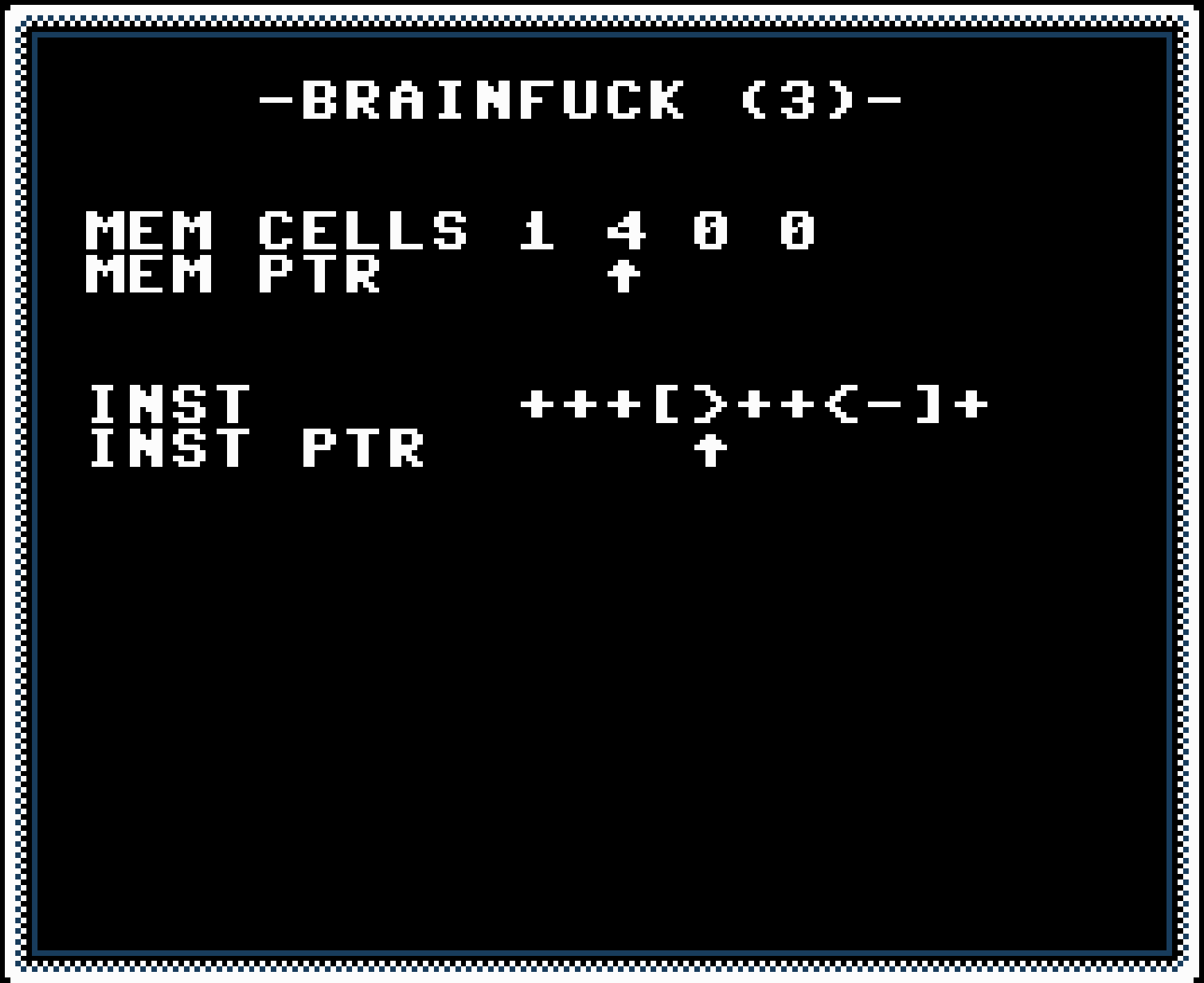
B - PREV A - NEXT



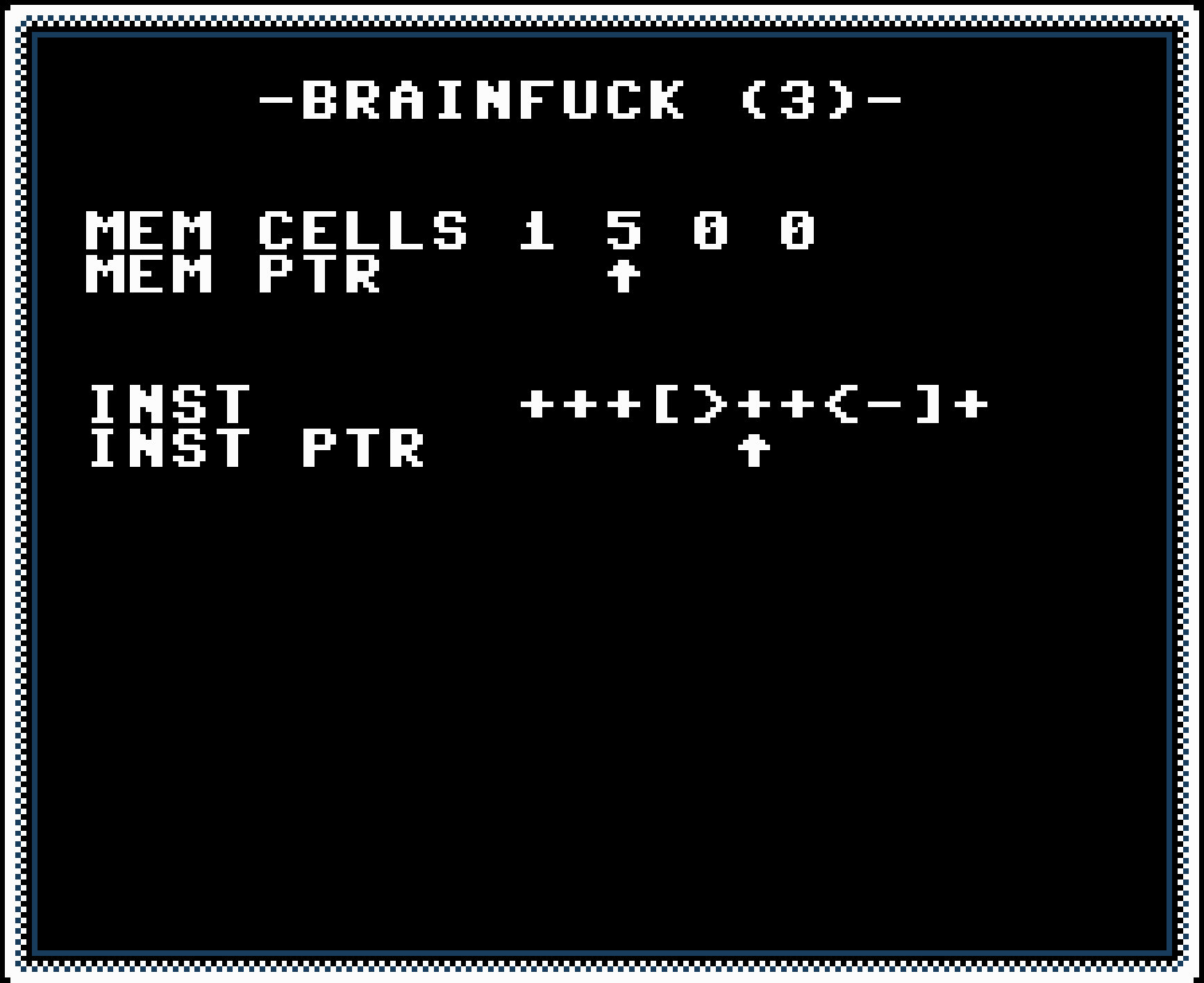
0 - PREV 0 - NEXT



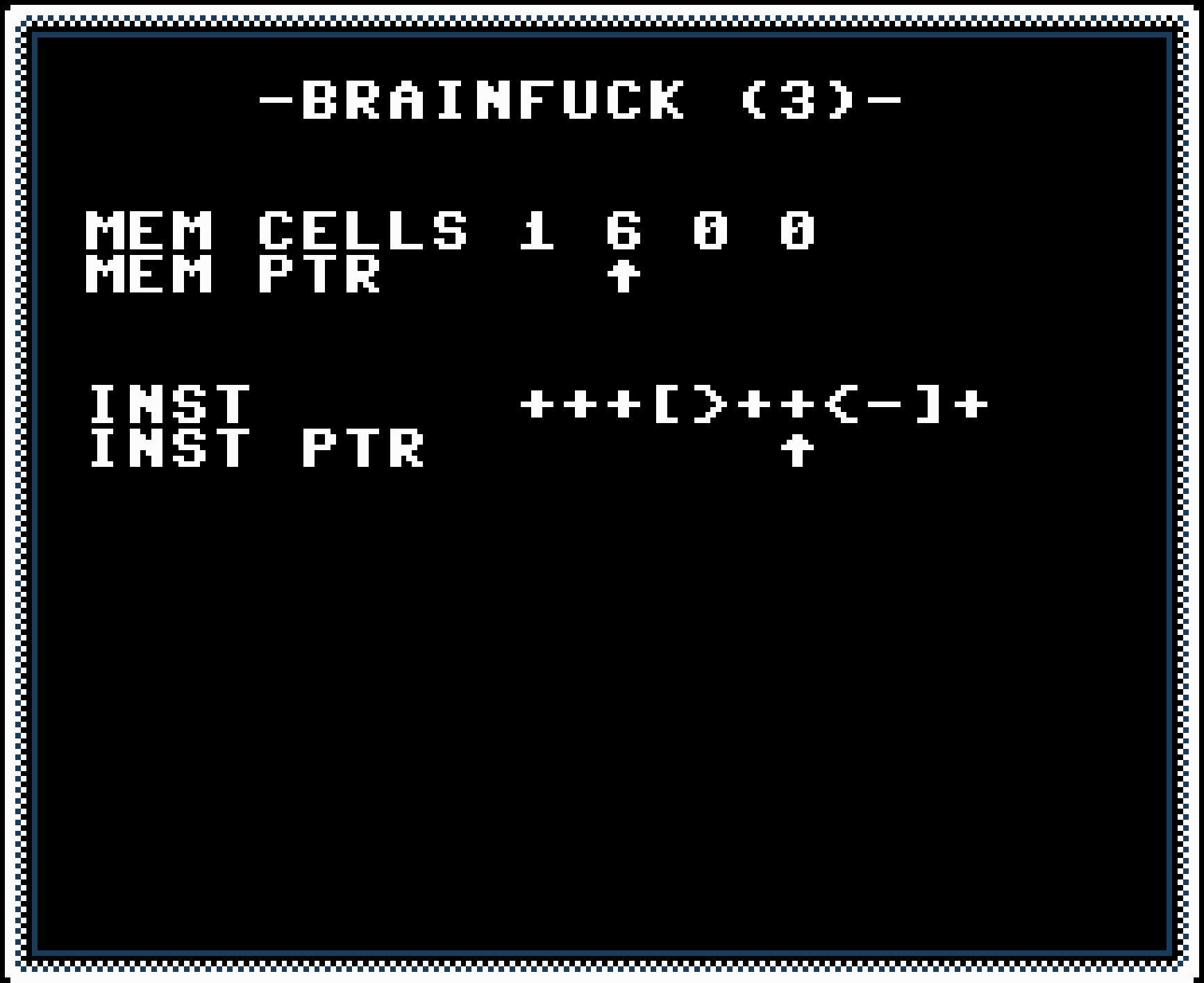
B - PREV A - NEXT



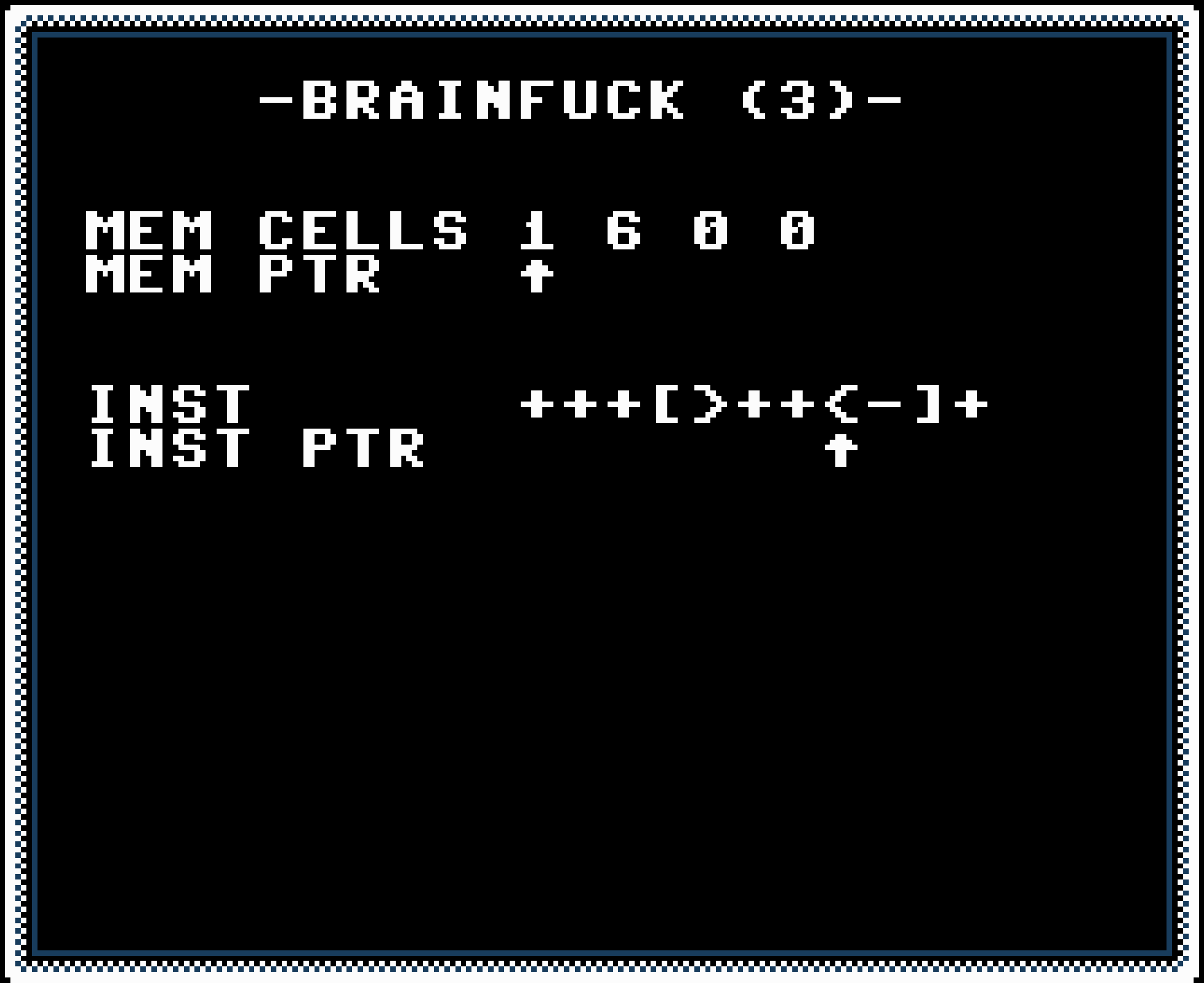
B - PREV A - NEXT



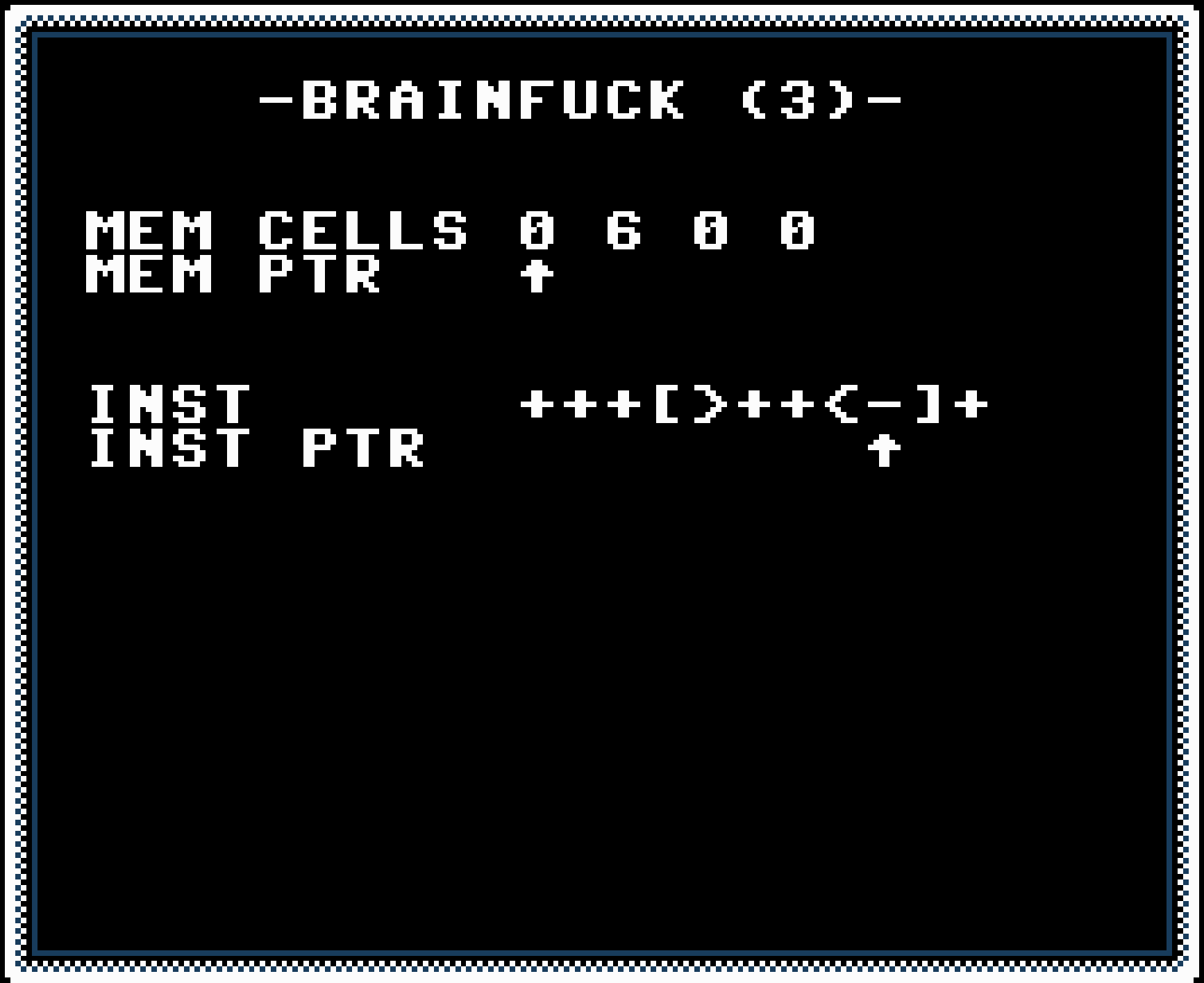
B - PREV A - NEXT



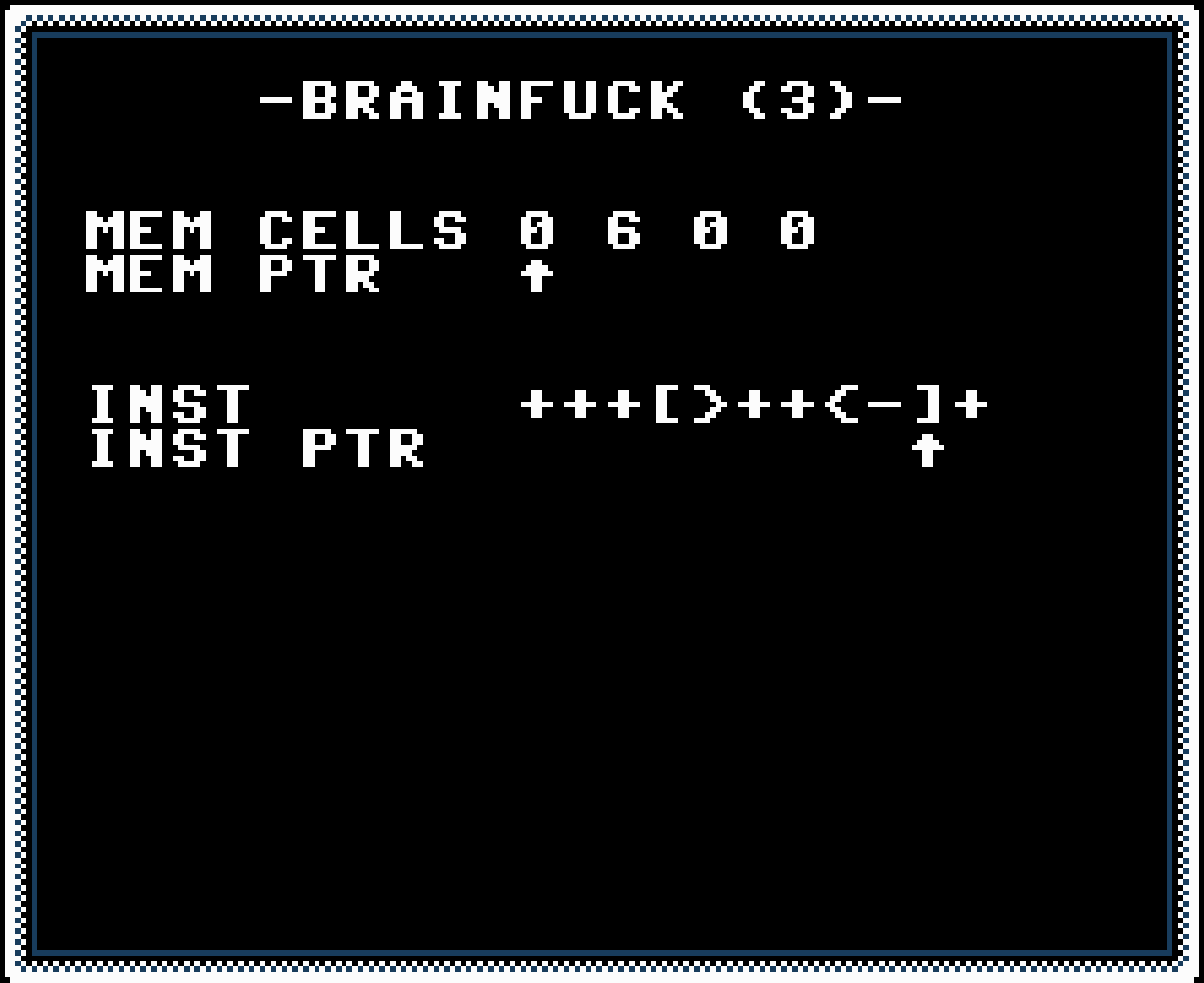
B - PREV A - NEXT



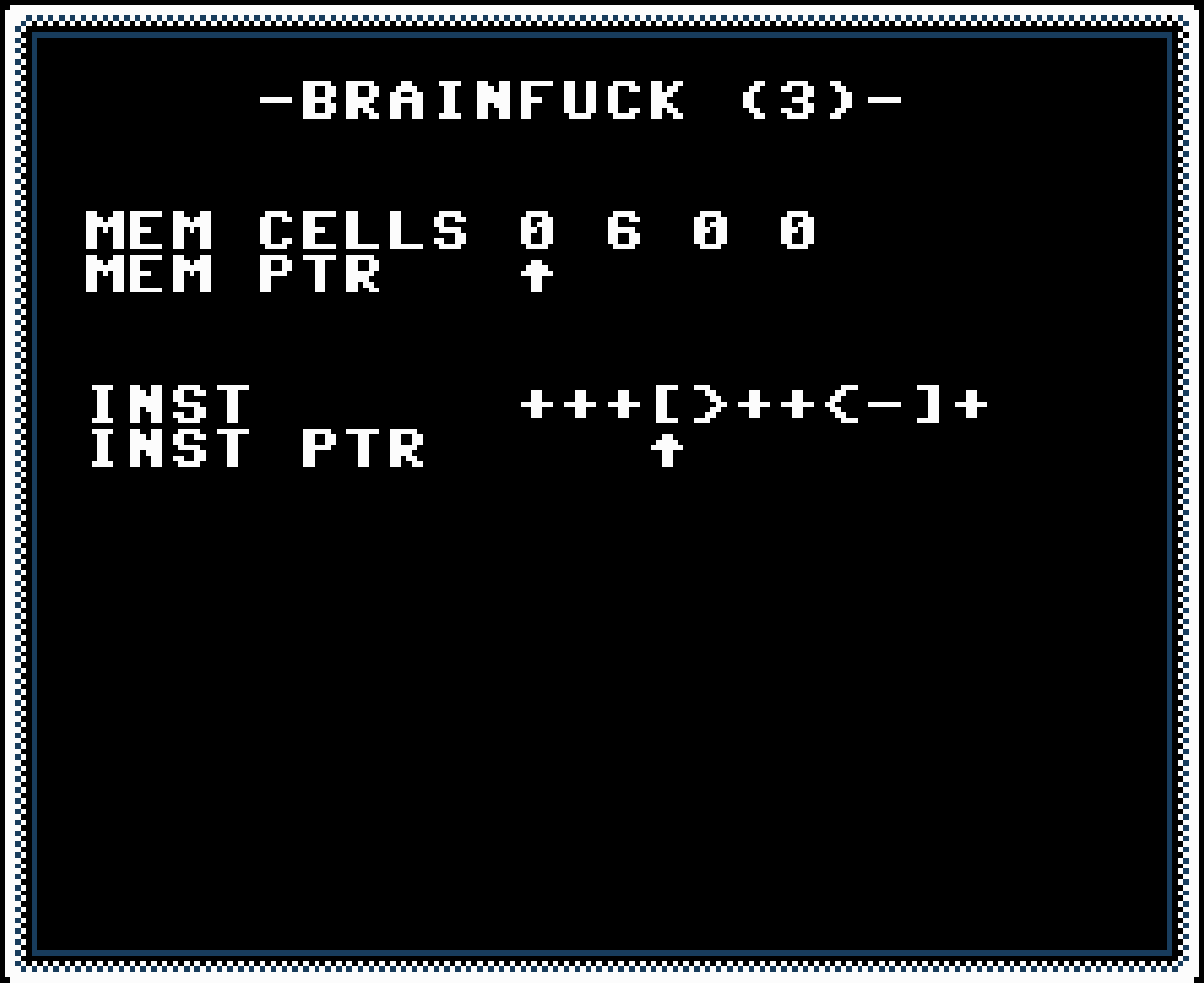
0 - PREV 0 - NEXT



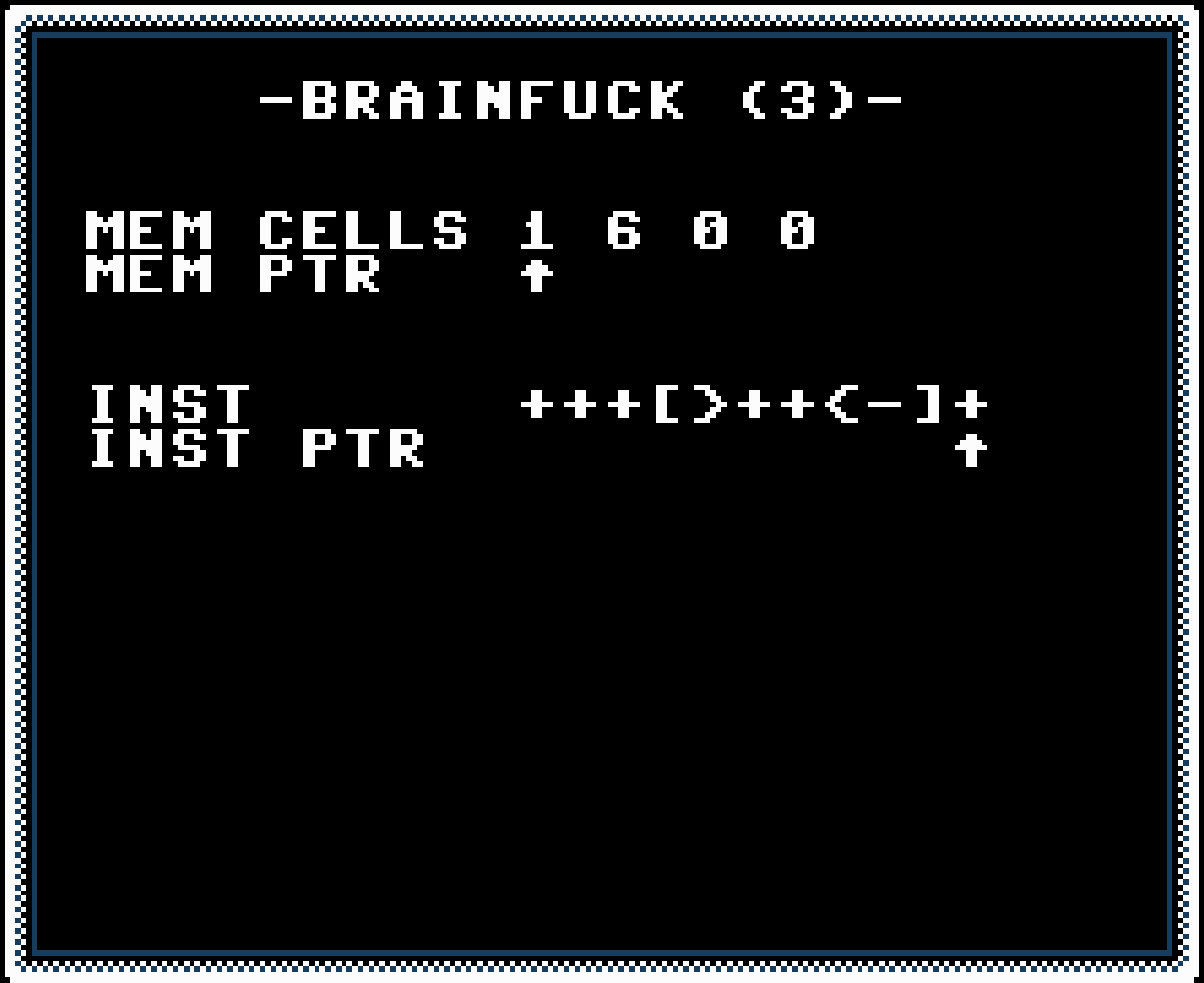
B - PREV A - NEXT



B - PREV A - NEXT



B - PREV A - NEXT



B - PREV A - NEXT

-BRAINFUCK (4)-

- EXTRA DATA MIGHT HAVE INSTRUCTIONS
- TO COMMENT EXTRA DATA OUT, WRAP IT IN SQUARE BRACKETS WHEN MEM CELL VALUE IS 0

```
[[]++>] ++. [-][>+]
```

-STRICT START FILE DATA-

- NES ROM FILE ALREADY A STRICT START FILE
- PRG AND CHR ROM DATA CAN HAVE UNUSED SPACE AT BEGINNING THOUGH
- THIS ALLOWS FOR 2 MORE POLYGLOT FILES!

B - PREV A - NEXT


-BITMAP IMAGE-
◦ STRICT FILE BEGINNING
◦ SMALL BITMAP IMAGE CAN FIT AT THE START OF OUR 32 KB PRG ROM DATA

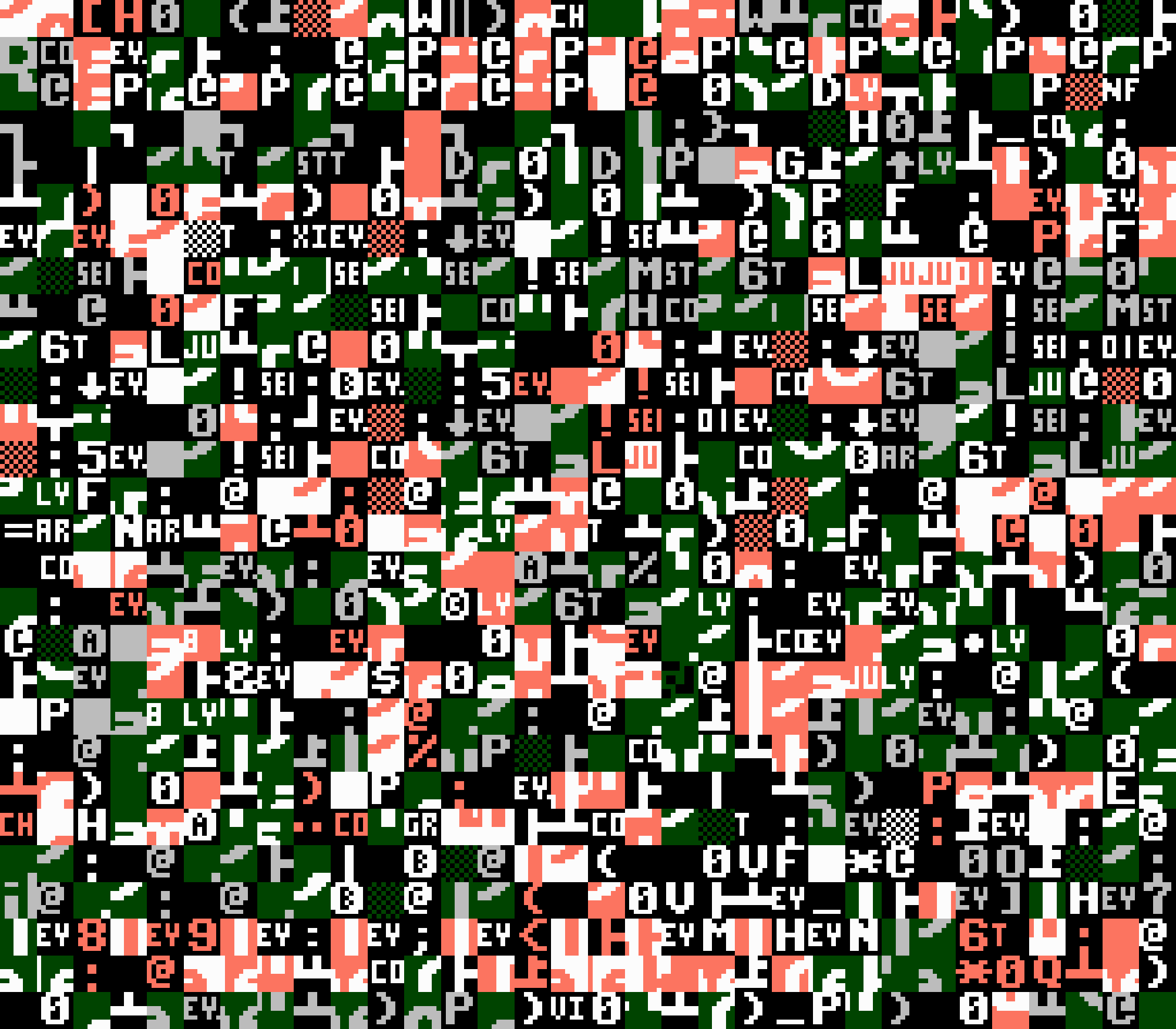
B - PREV A - NEXT

-NES-NROM-128 ROM-

- STRICT FILE BEGINNING
- 16 B INES HEADER
- 16 KB PRG ROM
- 8 KB CHR ROM
- FITS AT THE START OF OUR 32 KB CHR ROM DATA
- MAKE SURE PRG DATA AVOIDS PATTERN TABLE

B - PREV A - NEXT

B - PREV A - CRASH



```
$ unzip hopexii.nes
Archive:  hopexii.nes
   creating: zip/
  inflating: zip/braingoo.go
  inflating: zip/nrom-ines-prg-chr-split.py
  inflating: zip/README.txt
$
```

```
$ unrar x hopexii.nes

UNRAR 5.30 beta 2 freeware      Copyright (c

Extracting from hopexii.nes

Creating    rar
Extracting  rar/resume.txt
All OK
$
```

```
$ 7z -t7z x hopexii.nes

7-Zip [64] 9.20  Copyright (c) 1999-2010 Igo
p7zip Version 9.20 (locale=en_US.UTF-8,Utf16

Processing archive: hopexii.nes

Extracting  7z/hope.txt
Extracting  7z

Everything is Ok

Folders: 1
Files: 1
Size:       3040
Compressed: 65552
$
```


hopexii.nes as HTML File
GAME GENIE
BRAINFUCK
NES GAME GENIE
ENCODER/DECODER
GAME GENIE CODE
DECODE
ADDRESS
VALUE

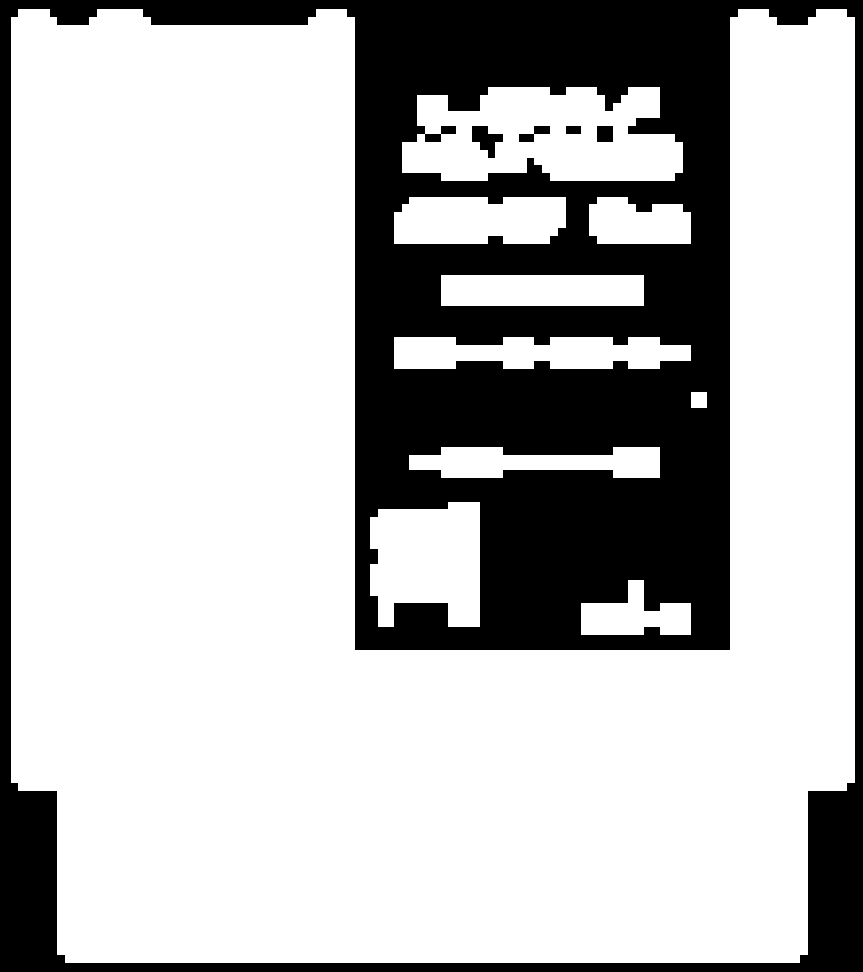

GAME GENIE
BRAINFUCK
BRAINFUCK
INTERPRETER
hopexii.nes
CHOOSE FILE
INTERPRET

hopexii.nes as Brainfuck File

OUTPUT

(2003 - 2017)
#TrevorForget

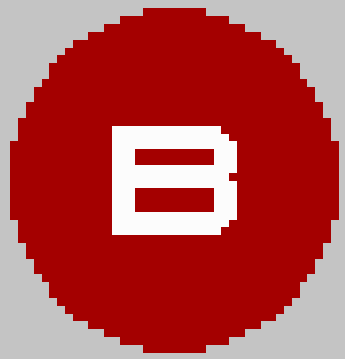
prg.bin as BMP File



chr.bin as NES ROM File

CHRUTH FABIAN

PRESSING BUTTONS

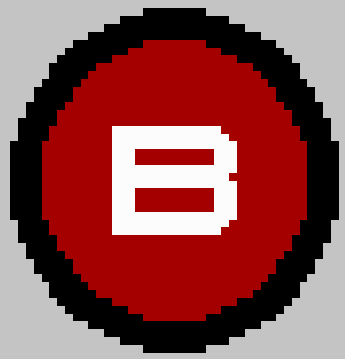


CHRUTHFABIAN.COM

CHRUTH FABIAN

PRESSING BUTTONS

REFLECTIONS ON HOPE

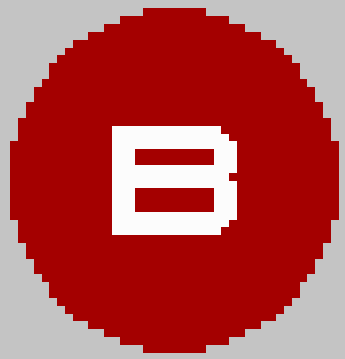


CHRUTHFABIAN.COM

CHRUTH FABIAN

PRESSING BUTTONS

A QUARTER WELL SPENT



CHRUTHFABIAN.COM