PowerPC disassembler

A cross-disassembler targeted for PowerPC 601 (and higher) and running on 680x0 Macintosh computers.

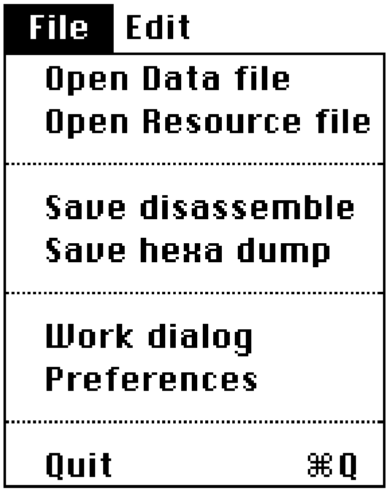
PowerPCdisas is an application to disassemble code for PowerPC microprocessor. The application converts a stream of number in a program (the code) into a text of mnemotechnic instructions defined by Motorola, the maker of the PowerPC microprocessor. The text can then be read to understand the program.

The PPCdis folder

This document is the English version of the user's guide in the PPCdis folder. The folder holds three files: PowerPCdisas.French- the French documentation, PowerPCdisas.English- the English documentation, and PowerPCdisas- the diassembler application. PowerPCdisas can be distributed freely, but please, keep the three files together.

The menus

The application can disassemble data files, ressource in a file or one instruction at a time. When you open PowerPCdisas, you see the usual menus **File** and **Edit**. The **File** menu hold 7 items:

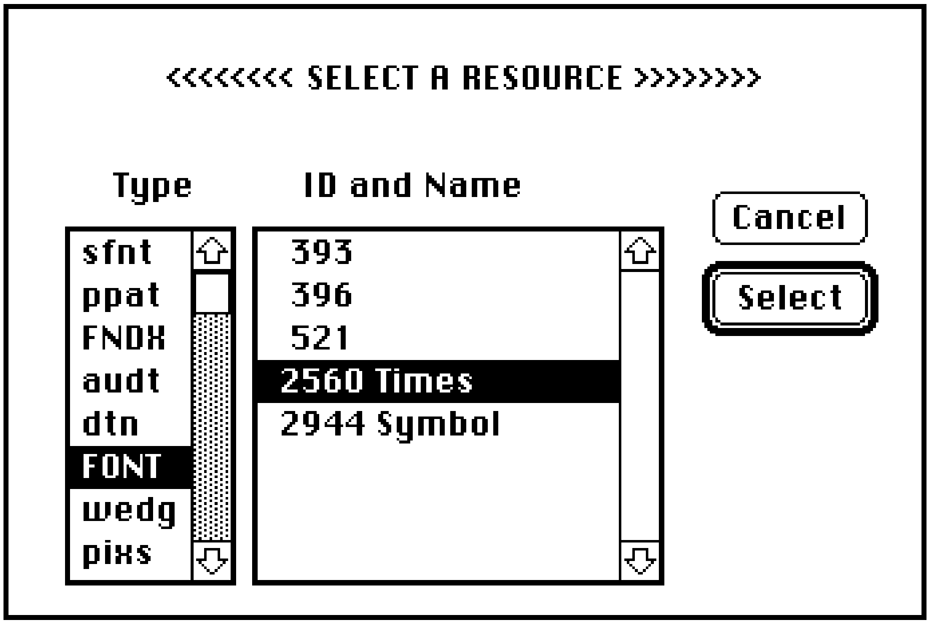


Open Data file

Shows the standard file selector box to open a data file to be disassembled.

Open ressource file

Shows the standard file selector box to open a resource file to be disassembled. A second dialog box is prompted to choose the resource.



You first select a file type in the left window. The right window then displays the number and the name for all resources of this type in the file. To disassemble a resource you must select both a type and a resource number.

Save disassemble

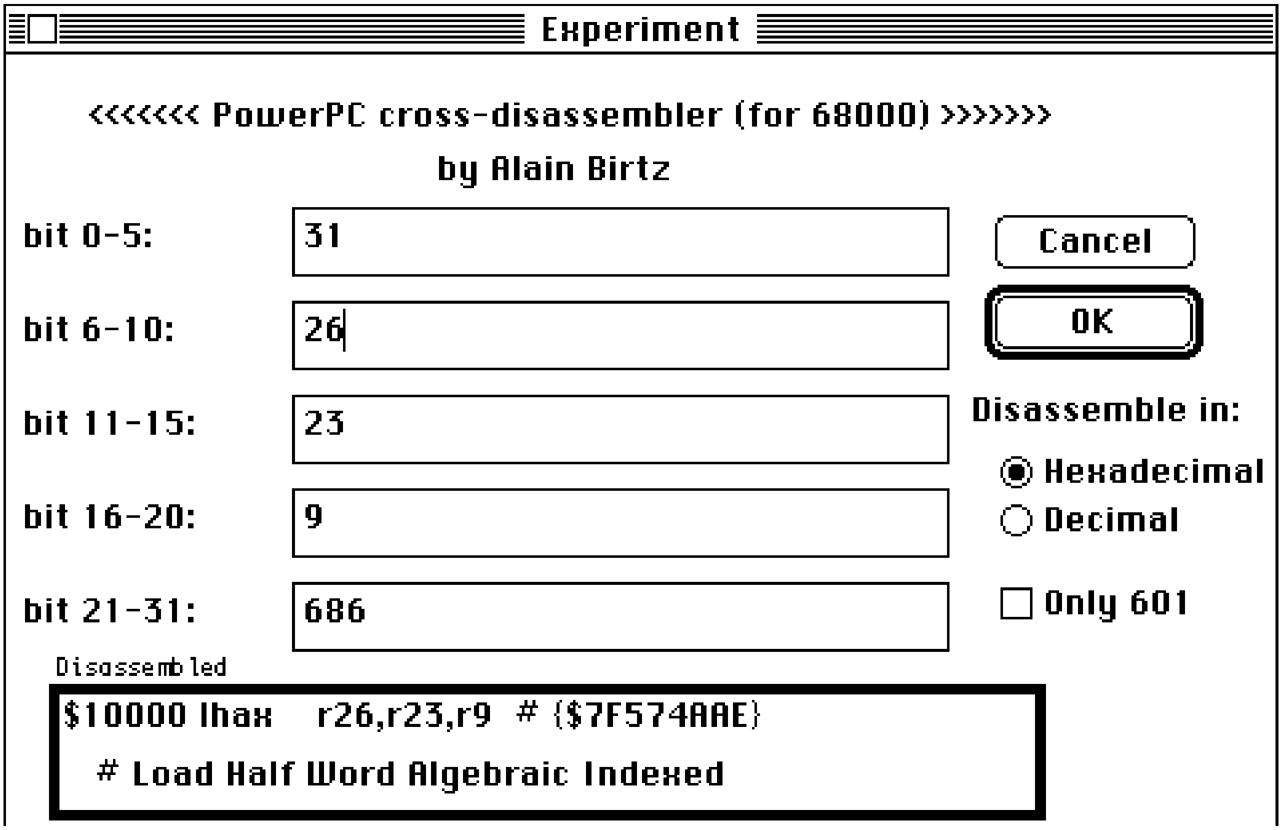
Shows the standard file selector box to save the text of the last disassembled file.

Save hexa dump

Shows the standard file selector box to save the text of the last file in hexadecimal and ascII form.

Work dialog

Shows the work dialog box to disassemble one instruction at a time. The first five edit fileds point out the binary field distribution of nearly all PowerPC instructions. You can enter a number in decimal or hexadecimal form. For the last form, you must add a leading **$**. The lower rectangle shows the result when the **Return** or **Enter** keys are hit or when **OK** is used. The numbers displayed in this rectangle are in decimal or hexadecimal according to the state of the two radio buttons **Hexadecimal** and **Decimal**. The **Only 601** check box, if checked, forces disassemble for PowerPC 601 code only. Otherwise the code is disassembled for instructions not common to the 601, but defined in the Motorola manual (for 604 or 620 ?).



<<<<<<< PowerPC cross-disassembler (for 68000) >>>>>>>

by Alain Birtz

bit 0-5: 31

bit 6-10: 26

bit 11-15: 23

bit 16-20: 9

bit 21-31: 686

Disassemble in:

● Hexadecimal

○ Decimal

□ Only 601

Disassembled

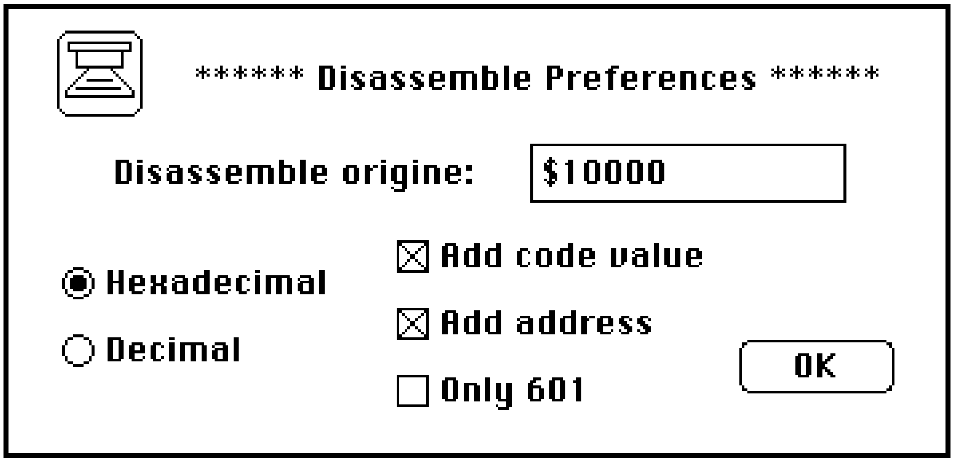
```
$10000 lhax   r26,r23,r9  # {$7F574AAE}
  # Load Half Word Algebraic Indexed
```

The Edit menu

You can use the edit menu as usual for cut and paste operations. For the **Hexa Dump** and **Disassemble** window you can select and copy only one line at a time. The usual command-c, command-x and command-v equivalent are also recongnized.

Preferences

Sow the preferences dialog box.



****** Disassemble Preferences ******

Disassemble origine: $10000

● Hexadecimal

○ Decimal

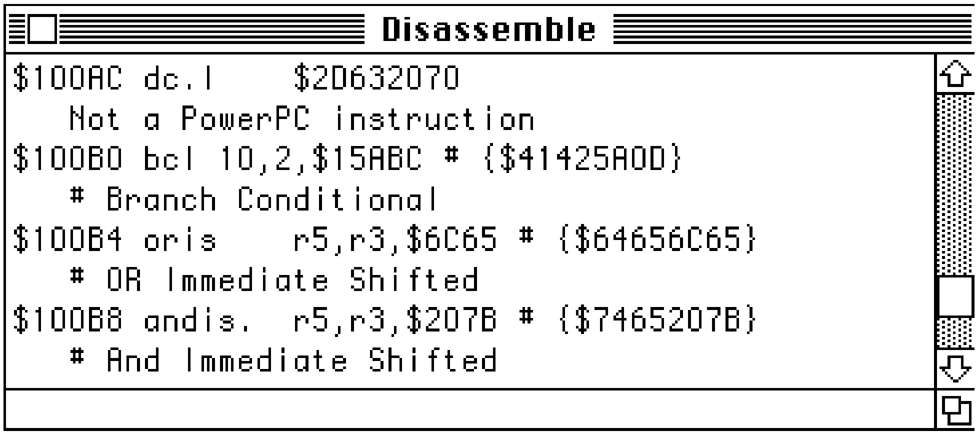
☒ Add code value

☒ Add address

□ Only 601

The two **Hexadecimal** and **Decimal** radio buttons and the **Only 601** check box, have the same meaning as above. The **Add code value** check box adds the instruction value between braces while the **Add address** check box adds the instruction address at the beginning of the line. In the **Disassemble origin** edit field you enter the address of the first instruction of the code to disassemble.

The disassemble window

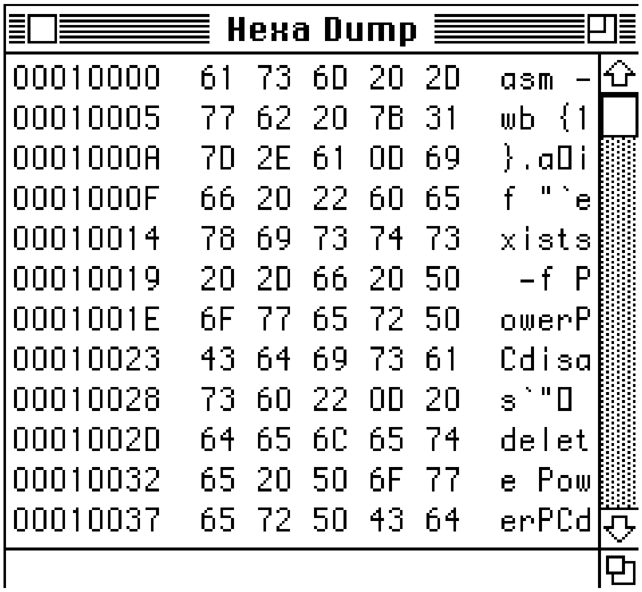


Disassemble

```
$100AC dc.l    $2D632070
   Not a PowerPC instruction
$100B0 bcl 10,2,$15ABC # {$41425A0D}
   # Branch Conditional
$100B4 oris    r5,r3,$6C65 # {$64656C65}
   # OR Immediate Shifted
$100B8 andis.  r5,r3,$207B # {$7465207B}
   # And Immediate Shifted
```

Each instruction is disassembled in two lines. The first one gives the mnemotechnic word of the instruction and the associate register or numeric value. The second line gives the meaning of the mnemotechnic word.

The hexadecimal dump window



```
00010000  61 73 6D 20 2D  asm -
00010005  77 62 20 7B 31  wb {1
0001000A  7D 2E 61 0D 69  }.a□i
0001000F  66 20 22 60 65  f "`e
00010014  78 69 73 74 73  xists
00010019  20 2D 66 20 50   -f P
0001001E  6F 77 65 72 50  owerP
00010023  43 64 69 73 61  Cdisa
00010028  73 60 22 0D 20  s`"□ 
0001002D  64 65 6C 65 74  delet
00010032  65 20 50 6F 77  e Pow
00010037  65 72 50 43 64  erPCd
```

The dump window runs in connection with the previous one, but the code is shown in hexadecimal and ascII form.

Limitation

This disassembler has been built only from the Motorola manual. Actually there is no (available) computer using the PowerPC microprocessor, and no PowerPC 601 assembler, so I cannot check the integrity of the disassembler.

How to use

It will be not easy to get presently some native PowerPC code. However, to have an idea of how the disassembler works, open any CODE resource no. 1 of an application. Even if PowerPC and 680x0 have nothing in common, you can see many disassembled PowerPC instructions. The PowerPC and 680x0 codings are compact enough to show most of the PowerPC instructions.

Future developpement

If I can get any cross-assembler, I will make some strong tests for the disassembler. I will also be able to put local labels for branch instruction and use alternative names for most frequently used form of branches.

Bug Report

PowerPCdisas has been tested on Mac Si and Quadra. If you find any bugs, please leave me a message (the kind of computer you use, when this bug appears,...) on CompuServe:

[72467,2770]

or write to:

Alain Birtz
650 Grand St-Charles,
St-Paul d’Abbotsford
P.Q., Canada, J0E-1A0