PowerPC disassembler V. 2

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

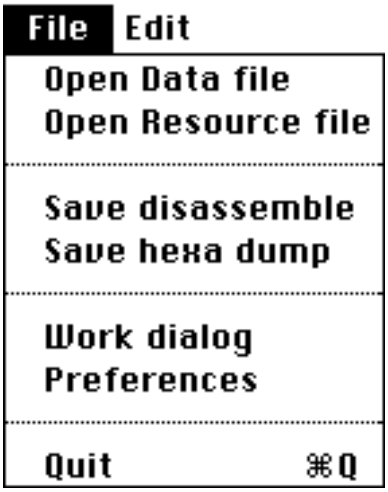
PowerPCdisas is an application to disassemble code for PowerPC microprocessor. The application converts a stream of numbers in a program (the code) into a text of mnemotechnic instructions defined by Motorola, the maker of the PowerPC microprocessor. The text can then be read to understand the program.

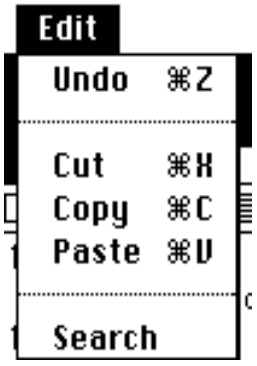
The PPCdis folder

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 holds 7 items:



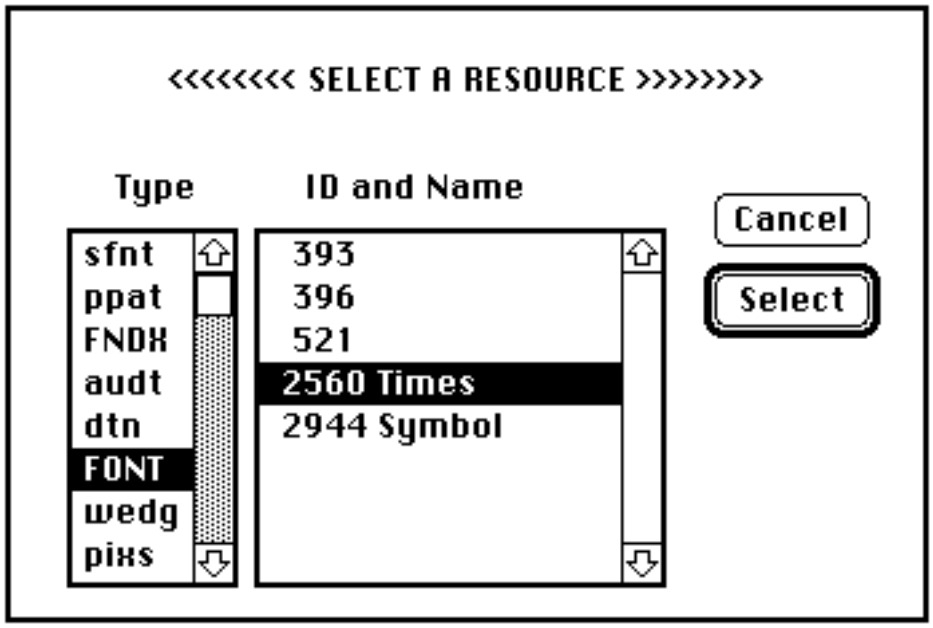


Open Data file

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

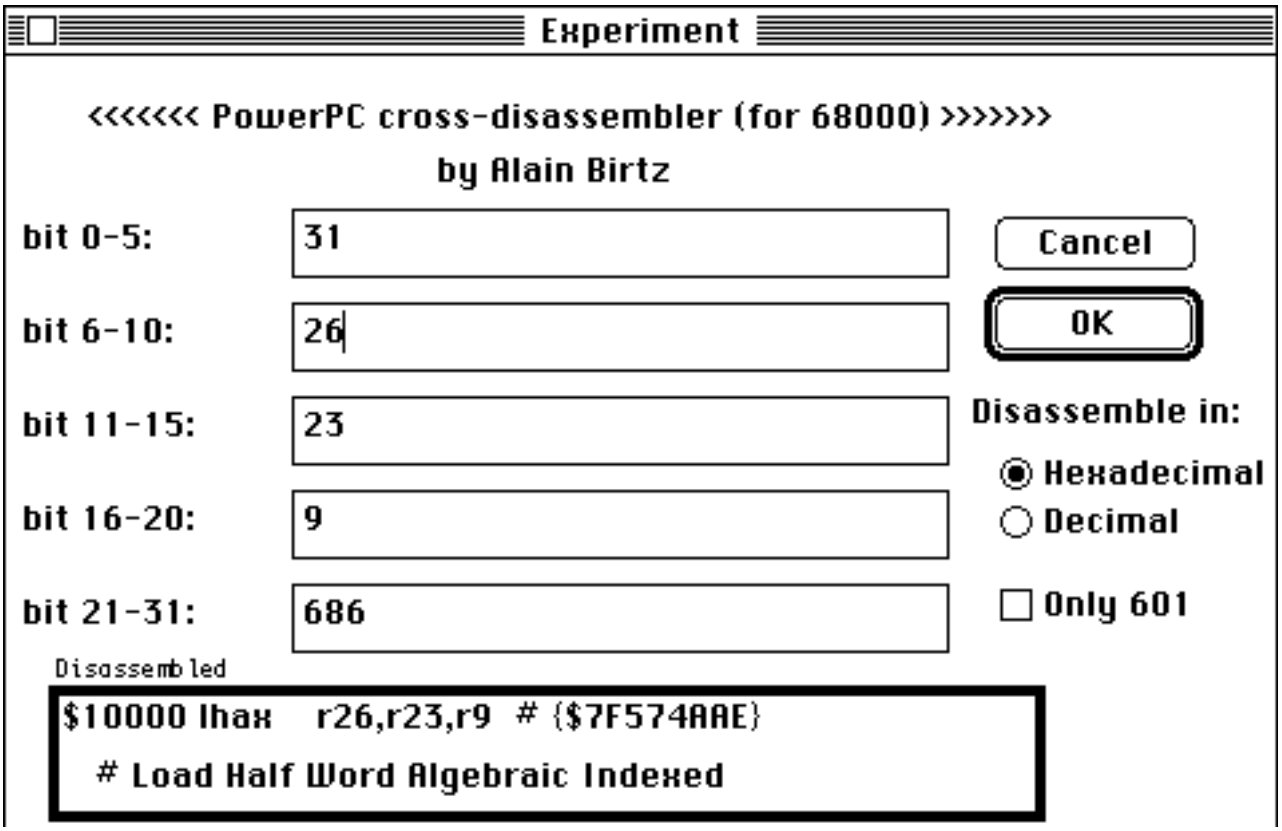
Shows the standard file selector box to save the text of the last disassembled file.

Save hexa dump

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

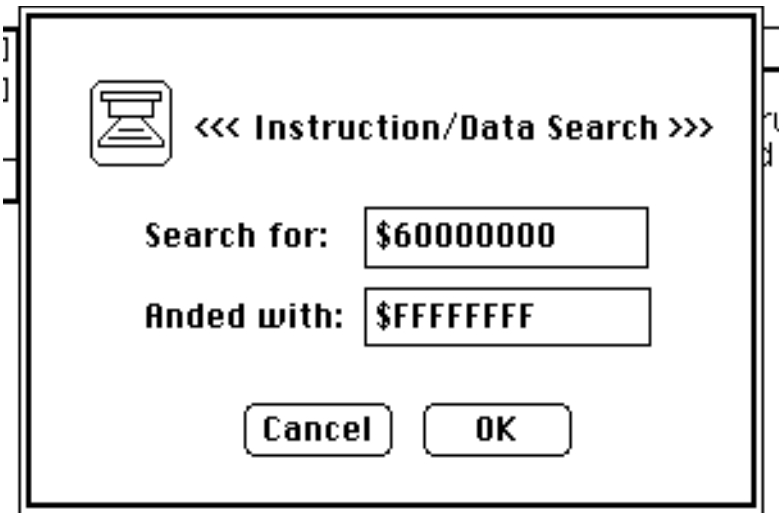
Work dialog

Shows the work dialog box to disassemble one instruction at a time. The first five edit fields 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 ?).

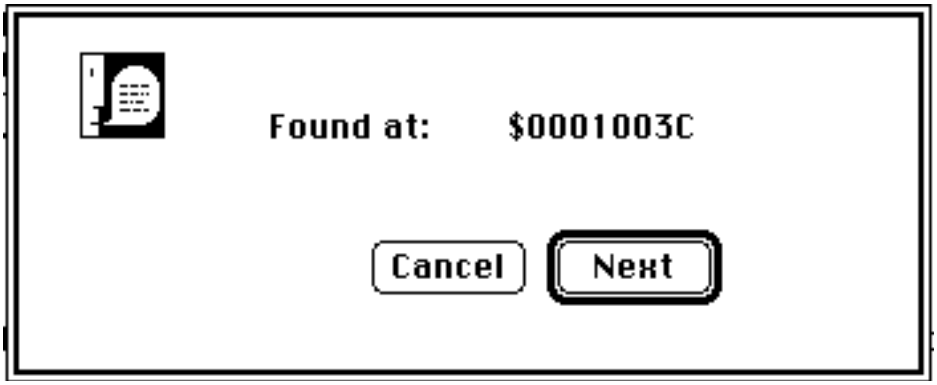


The Edit menu

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 and command-v equivalent are also recognized. The Search item can be use to search any 4 bytes word in the opened file or resource. You set the word to search and the mask bit in the following dialog box.



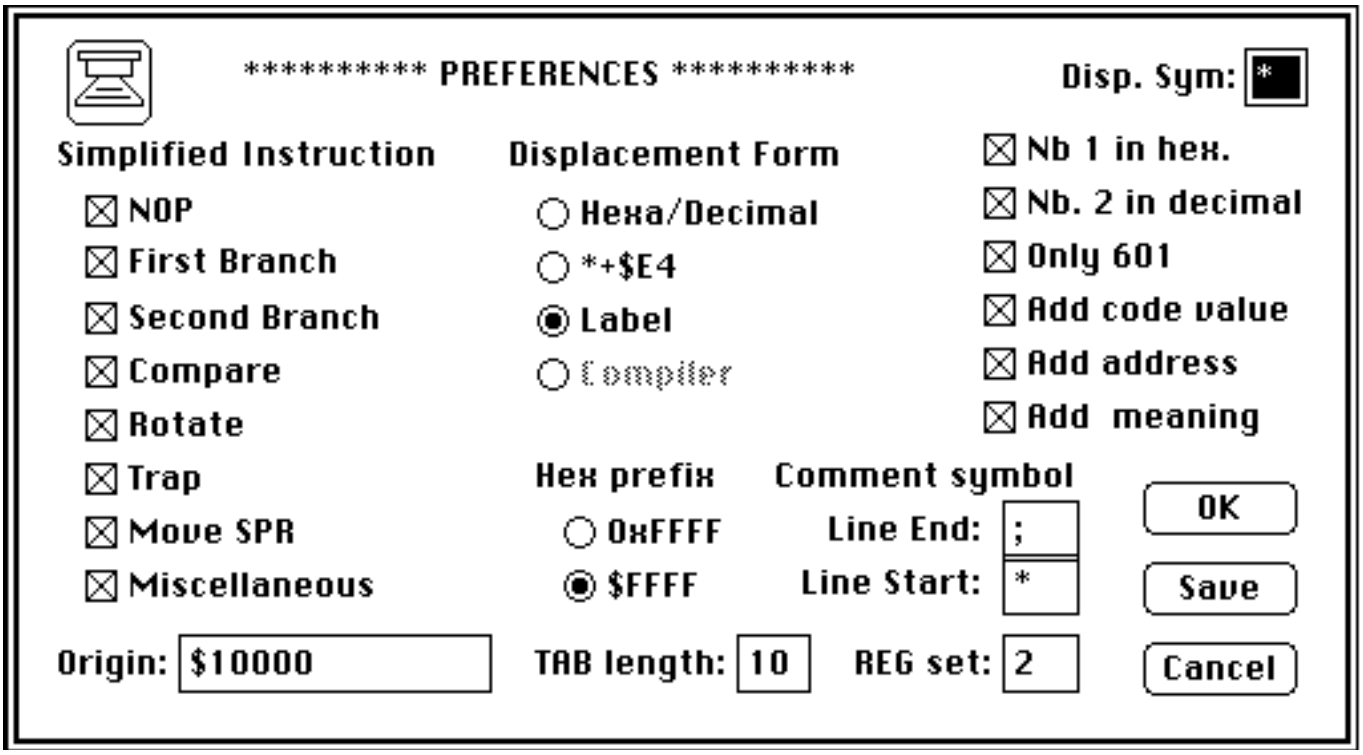
Every 4 bytes word are anded with the mask and then compared in the searched word. **Note:** the searched word is anded with the mask before the search begin. When a match occurs the following dialog box is displayed:



With the **Next** button, the search continues, while the **Cancel** button return to the menu.

Preferences

Show the preferences dialog box.



Simplified Instruction check box enable or disable the use of simplified PowerPC 601 instruction form in the disassembly.

NOP: replacement for **ori 0,0,0**. This instruction do nothing

First Branch: for all instructions **bc**, **bca**, **bclr** and **bcctr**

Second Branch: alternative simplified instructions for "branch if condition true" or "branch if condition false"

Compare: for **cmp**, **cmpl**, **cmpi**, **cmpli** instructions

Rotate: for **rlwnm**, **rlwinm**, **rlwimi** instructions

Trap: for **tw** and **twi** instructions

Move SPR: for **mtspr** and **mfspr** instructions

Miscellaneous: for **addi**, **addis** with first operand equal to r0 and **or**, **nor** with last two operands being equal (**mr**, **not**)

Note: Use the **s** key to turn ON/OFF the simplified form

Displacement Form radio-buttons set the form of the target operand field for branch instructions, and instructions address at the beginning of the disassembled line.

Hexa/Decimal: operands and address are shown as numbers (hexadecimals, or decimals, according to the **NB 1 in hex.** check box)

***+$E4**: operands are shown as relative displacement to PC (displacement in hex, or deci. according to the **NB 1 in hex.** check box and PC displacement symbol as defined in the **Disp. Symb.** edit field)

Label: operands and address are shown as label like LR_23 (for label referenced by instruction setting the LK bit: relative displacement), LA_23 (for label referenced by instruction clearing the LK bit: absolute displacement) and LB_23 (for label referenced by instruction of both type)

Compiler: not implnated in this version

Note: Use the * key to rotate between displacement form

Hex Prefix radio-buttons determine if hexadecimal numbers must begin by **$** or **0x**

Comment Symbol edit field set the symbol used for comments area

Line Start: for 68K, a complete line of comment must begin by *, Power PC use **#**

Line End: for 68K, a comment at the end the line begin by a semi colon, PowerPC use **#**

Origin hold the address of the first instruction of the code to disassemble

Tab Lengh hold the length of the tabulation between disassembled fields

Register Set this edit field determine which register name set must be used:

set 0: r0, r1, r2,..., fr0, fr1,...

set 1: GPR0, GPR1, GPR2,..., F0, F1,...

set 2: R0, SP, RTOC,..., FP0, FP1,... (standard Apple)

Note: Use the **r** key to rotate between set

Nb 1 in hex. check box, when checked, display address, displacement, and immediat value in hexadecimal. Otherwise these numbers are shown in decimal. **Note**: the **n** key can be used to toggle between the two forms

Nb 2 in decimal check, when checked, display small numbers like the mask and bit fields in the rotate and shift instructions, in decimal. Otherwise these values are shown in hexadecimal.**Note**: the **n** key can be used to toggle between the two forms

Only 601 check box, when checked, restrict the disassembly to PowerPC 601 only. Otherwise, 64 bits instructions are also disassembled

Add code value check box, when checked, add hexadecimal code, between braces, in the comment field

Add address check box, when checked, add instruction address (or label) at the beginning of the line.

Add meaning check box, when checked, add a second line of comments. This line gives the meaning of the mnemotechnic word

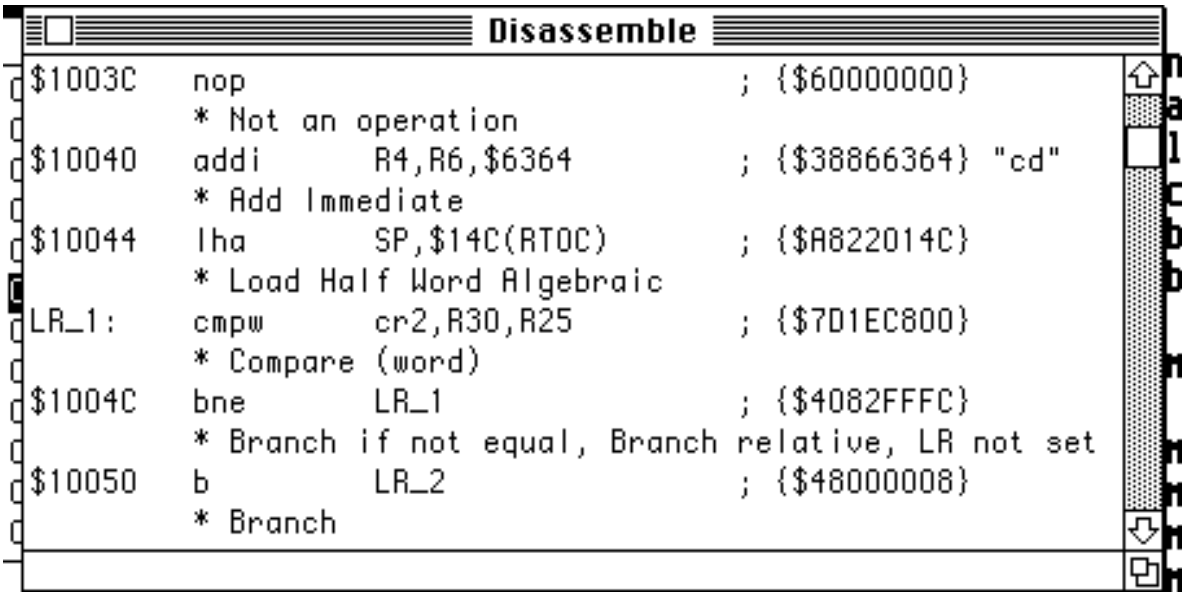
Disp. Symb this edit field hold the symbol used as PC reference in branch instruction. In 68K this symbol is *, while in PowerPC the symbol is $

Save button to close the dialog, change the setup, and save the setup for the next time

OK button to close the dialog, change the setup, but do not save the setup

Cancel button to close the dialog without doing any change

The disassemble window



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.

Keyboard shortcut

Command C copy the selected line to the clipboard

Command W close window and dialog

Up arrow scroll one line down

Down arrow scroll one line up

Shift Up arrow or **Page Down** scroll one page down

Shift Down arrow or **Page UP** scroll one line up

Home go to the start of the disassembly

END go to the end of the disassembly

S or **s** to turn ON/OFF the simplified form

R or **r** to rotate between register name set

N or **n** to change number from decimal to hexadecimal or vice-versa

f alignement key: add 2 to the address of the first byte of the segment to disassemble

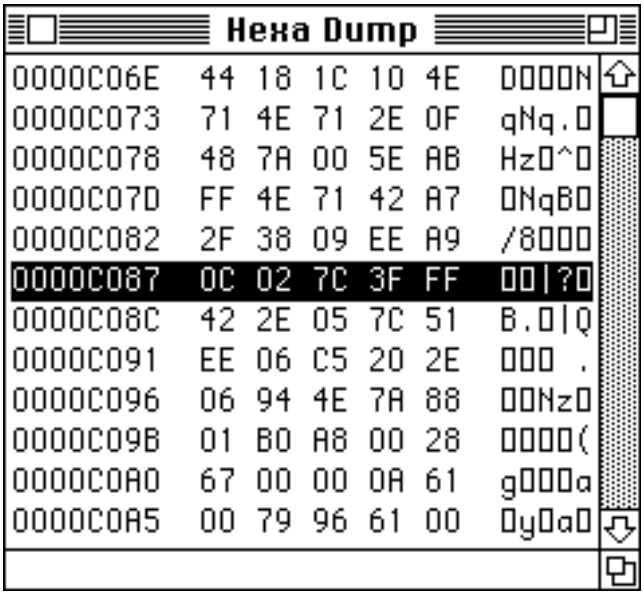
b alignement key: substract 2 to the address of the first byte of the segment to disassemble

F alignement key: add 1 to the address of the first byte of the segment to disassemble

B alignement key: substract 1 to the address of the first byte of the segment to disassemble

WARNING F and B key must be not used on the 68000 computer since this processor do not support word misalignement, and will generate a bus error (OK for 68020, 68030 et 68040)

The hexadecimal dump window



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

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