

M A D 8

UN DÉSAMBLEUR POUR 8008

JÉRÔME CHAILLOUX

ARTINFO/MUSINFO #28

1978

1978

1978

1978

MADB un desassembleur pour 8008

M A D B

Jerome CHAILLOUX
Fevrier 1977

MADB est un desassembleur de rubans perfores hexadecimaux issus du micro-processeur 8008. Il permet d'obtenir des listases "en clair" de vos programmes a partir d'un ruban perfore. MADB fonctionne sur le T1600.

1.0 Les rubans hexadecimaux.

Les rubans hexadecimaux images-memoire sont produits au moyen des commandes W, E et N du moniteur 8008. Ces rubans ne contiennent que des caracteres imprimables et peuvent donc etre relus sur une TTY non connectee (TTY en mode local).

1.1 La commande N (null command)

syntaxe : .N

perfore une avance bande de 60 caracteres nulls (code 00).

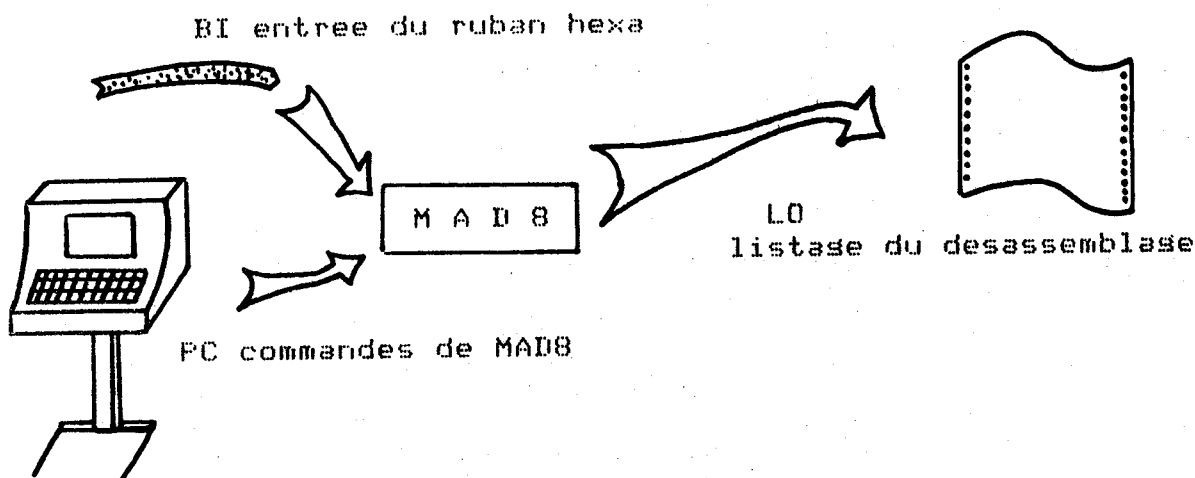
1.2 la commande W (write command)

syntaxe : .W adresse de debut , adresse de fin

perfore (dans le format decrit ci-dessous) l'image de la zone memoire commençant et se terminant aux adresses specifiées dans la commande. On peut emettre plusieurs commandes W a la suite pour obtenir, sur le meme ruban physique, les images de zones memoires non-contigües.

3.0 utilisation du desassembleur.

MAD8 est un utilitaire standard du T1600 qui utilise les differentes FUs :



3.1 activation de MAD8

*CALL MAD8 appel du programme MAD8. Si BOS/D imprime le message d'erreur ERB 06, le programme n'est plus sur le disque; il ne vous reste plus qu'a desassembler votre programme a la main ou a remettre MAD8 sur le disque.

*BI TR affectation du lecteur de ruban

*PC TK affectation du clavier TTY pour entrer les commandes de MAD8.

*LO LP affectation de l'imprimante pour le listase final.

3.2 commandes MAD8

*IMAD initialise MAD8 et lit le 1er ruban sur l'unité BI. Cette commande est obligatoire et ne doit être émise qu'une seule fois sous peine de perdre l'image mémoire qui avait été créée.

ou

- MAD8 ne peut simuler que les 8 kers du 8008. Si vous voulez desassembler des programmes en REPR0M (i.e des programmes dont l'adresse est plus grande que 2000 hexa), vous pouvez specifier dans la commande la 1ere adresse a simuler.
- *IMAD, hhhh** Cette deuxieme forme n'est donc pas a utiliser pour des programmes en RAM.
- *CMAD** permet de lire d'autres rubans sans reinitialiser le systeme, si votre programme se trouve sur plusieurs rubans perfores. Cette commande peut etre emise plusieurs fois.
- *MMAD** marque l'image memoire. On suppose que la premiere adresse du programme (son adresse de lancement) a ete lue sur le bloc fin de ruban du dernier ruban lu.
- *MMAD, hhhh** marque l'image memoire a partir de l'adresse specifiee dans la commande. Cette commande peut etre emise plusieurs fois en particulier pour specifier les differentes adresses se trouvant dans une table de branchements indirects indexes.
- *LMAD** edite sur l'unite LO le resultat du desassemblage. Cette commande peut etre emise plusieurs fois pour obtenir plusieurs copies du desassemblage.
- *EOJ** fin d'execution de MAD8.

3.3 utilisation du disque

Le lecteur de ruban de la TTY est tres lent. Il est parfois avantageux de creer un fichier sur disque contenant l'image du ruban hexadecimal a desassembler ce qui evite de recharger le ruban apres chaque erreur.

Pour copier le ruban perfore sur disque, il faut utiliser l'utilitaire standard du T1600 : le FUP6.

***CALL FUP6** appel de l'utilitaire FUP6.

***INPUT, TR, PTAP** definition du support d'entree

*OUTPUT,nom-:I definition du fichier de sortie. L'extension
:I est reservee pour les fichiers hexa de
l'Intel.

*TRANSF effectue le transfert

*EOJ fin du travail

4.0 Exemples d'utilisation de MAD8

desassemble direct d'un ruban perforé :

*CALL MAD8 appel de MAD8.
*BI TR selection du lecteur en entree.
*LO LP selection de l'imprimante.
*IMAD initialisation et lecture
--- lecture du ruban ---
*MMAD marquage des instructions.
*LMAD listage de l'image memoire.
--- impression du resultat ---
*EOJ voila le travail

Exemple du desassemble complet du moniteur 8008.

*EOJ

*CALL FUP6 creation d'un fichier disque
*INPUT,TR,PTAP contenant le ruban hexa du moniteur.
*OUTPUT,MONIT-:I,D2
*TRANSF
--- lecture du ruban ---
*EOJ

*CALL MAD8
*BI MONIT-:I,D2
*PC TK
*LO LP
*IMAD,2000
*MMAD
*MMAD,38A3 marquage de tous les modules
*MMAD,39DE du moniteur.
*MMAD,3967
*MMAD,39A9
*MMAD,39D4
*MMAD,3A00
*MMAD,3A13
*MMAD,3A1A
*MMAD,3C43

```

*MMAD,3A45
*MMAD,3A5F
*MMAD,3A8B
*MMAD,3A91
*MMAD,3AF6
*MMAD,3B68
*MMAD,3BB7
*MMAD,3BD5
*LMAD

```

```

--- impression du desassemblage ---
*EOJ

```

5.0 Exemple de listage produit par MAD8.

0040	JMP	0703		0079	CPM
0043	LLI	32 2		007A	JFZ 007F
0045	LHI	00		007D	LAB
0047	LCI	01		007E	RET
0049	JMP	3D80		007F	DCL
004C	LLI	30 0		0080	DCB
004E	LHI	00		0081	JFS 0079
0050	LAM			0084	JMP 3C43
0051	INL			0087	LLI 33 3
0052	LBM			0089	LHI 00
0053	LMA			008B	LME
0054	LLB			008C	RET
0055	RET			008D	CPI 46 F
0056	CAL	004C		008F	RTZ
0059	LME			0090	CPI 54 T
005A	CAL	3DEB		0092	JFZ 3C43
005D	LAH			0095	LAI 20
005E	LBL			0097	LLI 33 3
005F	LLI	30 0		0099	LHI 00
0061	LHI	00		009B	ADM
0063	LMA			009C	LMA
0064	INL			009D	RET
0065	LMB			009E	CAL 00A7
0066	RET			00A1	LLI 33 3
0067			IN 41 A	00A3	LHI 00
0068			CFC 42 B	00A5	LEM
0069			IN 43 C	00A6	RET
006A			JMP 44 D	00A7	CPI 43 C
006B			IN 45 E	00A9	RTZ
006C			JFZ 48 H	00AA	CPI 5A Z
006D			--- 4C L	00AC	LBI 08
006E			IN 4D M	00AE	JTZ 00BF
006F			IN 49 I	00B1	LBI 10
0070	CAL	3F44		00B3	CPI 53 S
0073	LBI	08		00B5	JTZ 00BF
0075	LLI	6F		00B8	LBI 18
0077	LHI	00		00BA	CPI 50 P
				00BC	JFZ 3C43
				00BF	LAB
				00C0	JMP 0097
				00C3	CPI 08
				00C5	JTZ 055E

00C8	ADE
00C9	ADI 7C
00CB	JMP 0553

0500	CAL 3CC7
0503	LBI 3A :
0505	CAL 3809
0508	CAL 0043
050B	LLI 30 0
050D	LMD
050E	INL
050F	LME
0510	CAL 3CC7
0513	CAL 004C
0516	CAL 3DFB
0519	CAL 3F44
051C	CPI 24 \$
051E	JTZ 3844
0521	CPI 42 B
0523	JFZ 0538
0526	CAL 3F44
0529	CAL 3F44
052C	CAL 3C4B
052F	CAL 0043
0532	CAL 0056
0535	JMP 0510
⋮	⋮
⋮	⋮
⋮	⋮

c'est sûrement
l'adresse d'implantation

c'est probablement
du programme

c'est probablement
des données