C T E I BP 41 83220 LE PRADET
RC Toulon 85 A 745 RM Toulon 332550060830 N° Siret 332 550 060 00013
Code APE 2914 Banque Populaire Le Pradet 88 21 026 958

MODE D'EMPLOI DU DESASSEMBLEUR

GENERALITES

Un désassembleur est un programme qui, à partir du code machine représenté sous forme binaire, est capable de reconstituer la suite de mnémoniques correspondants. Il permet donc de re créer le fichier source d'assemblage d'un programme à partir du programme objet. Outre l'intéret 'que cela présente pour toute personne désireuse de savoir comment fonctionne un programme, cela permet aussi de modifier un programme désassemblé pour l'adapter exactement à ses besoins.
Aussi performant qu'il soit, un désassembleur ne peut cependant pas faire de miracle et il faut bien souvent l'aider dans son travail. De l'efficacité de la collaboration entre l'utilisateur et le désassembleur dépend l'efficacité du désassemblage. Cette collaboration efficace ne peut se concevoir que de la part d'un utilisateur ayant un minimum de notions relatives au langage machine du microprocesseur concerné.
Pourquoi faut il aider un désassembleur? Tout simplement parce que la zone mémoire ou le fichier que vous lui donnez à traiter ne contient pas qu'une suite de codes machines 6800 ou 8809 (car si tel était le cas il saurait faire tout seul) mais renferme également des zones de constantes, des zones de variables, des textes, etc.... Il faut donc lui signaler la présence de ces zones afin qu'il puisse faire du travail correct. Comme, à priori, vous ne savez pas toujours où elles se trouvent, vous allez devoir faire plusieurs "passes" de désassemblage pour cerner leurs positions. Nous allons voir que tout cela est très facile à faire avec DESASS.

LA DISQUETTE CI JOINTE

La disquette ci jointe supporte cinq fichiers:
- DESASS CMD qui est le désassembleur proprement dit
- DISLBL00.BIN qui est un fichier d'étiquettes standards du DOS 6800. Ce fichier est appelé automatiquement par DESASS lors des désassemblages 6800 si nécessaire.
- DISLBL09.BIN qui est la même chose que DISLBL00 mais pour le DOS 6809 et les désassemblages 6809.
- DISLBL00.TXT et DISLBL09.TXT qui sont les fichiers sources des deux précédents afin de vous permettre de les modifier ou de les compléter si vous le jugez utile.

AVANT D'UTILISER VOTRE DESASSEMŒLEUR, FAITES AU MOINS UNE COPIE DE SAUVEGARDE DE LA DISQUETTE CI JOINTE POUR EVITER TOUT PROBLEM EN CAS DE FAUSSE MANOEUVRE DE VOTRE PART.

LES POSSIBILITES DE DESASS

DESASS est un désassembleur de haut de gamme qui dispose des possibilités et particularités suivantes:
- Il fonctionne sur les systèmes TAV09 ou TAV85.
- Il peut désassembler des programmes 6800 ou 6809 quelle que soit leur implantation mémoire car il travaille directement avec les fichiers disques contenant ces programmes.
- Même si le désassemblage n'est pas correct, le fichier source produit peut etre ré assemblé pour donner un programme identique à celui désassemblé.
- Il produit automatiquement des étiquettes pour toutes les références mémoires. Ces étiquettes sont définies par une suite de directives EQU regroupées automatiquement en début de programme.
- Il connait toutes les étiquettes standards du DOS et peut prendre en compte tout fichier d'étiquettes que vous pourriez etre amené à créer.
- Tout bloc de données d'un programme à désassembler qui n'est pas du code machine peut etre traité comme étant: une suite de constantes sous forme d'octets, de mots, de chaines de caractères ou d'adresses. DESASS produit automatiquement sur le listing les directives FCB, FDB ou FCC selon le cas.
- Ces zones particulières peuvent etre spécifiées en temps réel lors du désassemblage ou etre lues dans un fichier dit de commande qui vous épargne de multiples frappes lors des désassemblages longs.
- Le listing de désassemblage peut etre paginé, recevoir des numéros de ligne et etre vu sur l'écran ou dirigé vers un fichier disque.

TERMINOLOGIE

DESASS utilise un certain nombre de types de fichiers pour travailler. Afin que ce manuel soit aussi précis que possible, voici les définitions de ces derniers ainsi que les noms qui leur seront donnés tout au long de cette notice.
- Fichier d'entrée (Input File) est le fichier binaire contenant le programme à désassembler.
- Fichier de sortie (Output File) est le fichier créé par DESASS pour recevoir le listing source de désassemblage.
- Fichier de commande (Command File) est un fichier texte optionnel qui contient les définitions des diverses zones de constantes du programme à désassembler.
- Fichier d'étiquettes (Label File) est un fichier binaire qui contient les définitions et adresses des étiquettes de votre choix. Par défaut, les fichiers DISLBLO0 (pour un désassemblage 6800) ou DISLBL09 (pour un désassemblage 6809) sont utilisés.

UTILISATION DU DESASSEMLEUR

La syntaxe la plus générale qui soit pour appeler le désassembleur est la suivante:

+++DESASS Fichier d'entrée Fichier de sortie +options +Fichier de commande.

Par défaut, tous les fichiers sont recherchés sur le disque de travail, sauf le désassembleur qui, comme toute commande DOS, doit résider sur le disque système. Hormis le Fichier d'entrée dont la présence est obligatoire, toutes les autres rubriques de la ligne ci avant sont facultatives.

L'extension par défaut du Fichier d'entrée est .CMD. Bien sur, il est possible de ne pas utiliser ces choix par défaut; ainsi:

+++DESASS 0.PROGRAM.BIN ferait désassembler le programme appelé PROGRAM.BIN, placé sur le disque 0.

Si aucun nom de fichier de sortie n'est indiqué mais qu'une sortie sur disque soit demandée, le fichier créé aura le même nom que le fichier d'entrée mais avec l'extension TXT.
Si le Fichier de sortie existe déjà, DESASS demandera s'il peut l'effacer ou non sous la forme:
Output file exists - Delete it (Y-N) ? Le fait de répondre Y le fera effacer tandis que N interdira son effacement et arretera donc le désassemblage. '
Les options sont représentées par des lettres placées dans n'importe quel ordre, après le premier signe +, sans aucun symbole ou espace entre elles. Les différents choix possibles sont les suivants:
- A fait imprimer l'équivalent ASCII de chaque octet du programme désassemblé. Cela permet de retrouver très facilement les zones contenant des messages. Tout caractère ASCII non imprimable (code inférieur à 20) est représenté par un point '.'.
- B fait demander par DESASS les zones de constantes. Ce mode d fonctionnement est décrit en détail ci après.
- D interdit la création d'un fichier de sortie sur disque MEME si un nom est spécifié sur la ligne d'appel de DESASS.
- G interdit l'affichage sur le listing de désassemblage de plus de 4 octets dans les zones contenant des FCC, FCB et FDB ce qui fait gagner de la place pour les programmes avant de très longues zones de constantes.
- L interdit la sortie d'un listing de désassemblage sur l'écran ou l'imprimante du système.
- N fait générer des numéros de lignes sur le listing de désassemblage.
- P valide la pagination du listing de désassemblage. Un titre pouvant contenir jusqu'à 32 caractères vous est alors demandé. Ce titre sera affiché en haut-de chaque page.
- S permet de ne faire désassembler qu'un segment de programme ignorant tout le reste de ce dernier. Cette option est très utile pour le désassemblage de programmes très longs.
- Z demande un désassemblage 6800 au lieu de 6809 qui est la valeur prise par défaut.
- 0 à 3 indique sur quel lecteur DESASS doit lire le fichier DISLBLOX.BIN. Par défaut, ce dernier est lu sur le même disque que celui contenant DESASS mais, en précisant un numéro de 0 a 3

dans les options, il peut etre lu sur le disque de votre choix.

Le dernier élément de la ligne d'appel de DESASS est le fichier de commande. Le contenu de ce fichier est décrit en détail plus avant dans ce manuel. Il est pris par défaut sur le disque de travail et avec l'extension TXT. Son nom doit etre placé après un signe + se trouvant après toutes les lettres d'options. Si aucune option n'est spécifiée, son nom doit etre précédé de deux signes ++ (celui des options suivi de rien et celui du fichier).

Voici quelques exemples commentés d'appel du désassembleur:

+++DESASS PROG +DAN
Désassemble le programme PROG.CMD pris sur le disque de travail. Aucun fichier disque n'est créé (option D), l'équivalent ASCII de tous les octets est affiché (option A), les lignes du listing de désassemblage sont numérotées (option N).

+++DESASS O.TOTO l.SOURCE +ZLS
Désassemble le fichier TOTO.CMD pris sur le disque 0 et place le résultat du désassemblage dans le fichier SOURCE.TXT placé sur le disque 1. Le programme est en langage 6800 (option Z), aucun listing n'est envoyé sur l'écran du système (option L) et seul un segment de programme sera désassemblé (option S) dont l'adresse sera demandée avant désassemblage comme expliqué ci après.

+++DESASS PROG SOURCE +PN +COMPROG
Désassemble le fichier PROG.CMD pris sur le disque de travail et place le résultat dans le fichier SOURCE.TXT placé sur le disque de travail. Le listing sera paginé et numéroté (options P et N)

et un fichier de commande baptisé COMPROG.TXT pris sur le disque de travail sera utilisé.

DIALOGUE AVEC LE DESASSEMLEUR

Trois options, B, P et S conduisent DESASS à vous poser des questions avant qu'il puisse commencer à travailler. Nous allons voir la signification et la syntaxe de celles ci.

Si l'option« P est spécifiée, DESASS demande un titre sous la forme:
Title?
Ce dernier peut comporter jusqu'à 32 caractères (les caractères en excès sont ignorés) et doit etre terminé par un retour chariot.

Si l'option B est spécifiée, DESASS va vous demander de lui définir les différentes zones de constantes du programme à désassembler de la façon suivante:
Data Segment Type: Ascii, Byte, Label, Word, Reset, or Proceed?
Vous devez alors frapper une lettre et une seule parmi les suivantes selon ce que vous désirez préciser à DESASS. Toute frappe d'autre chose qu'une des lettres attendues fait poser à

nouveau la question.

- A déclare une zone de constantes comme contenant des codes ASCII. DESASS générera alors automatiquement des directives FCC suivies par les caractères ASCII correspondants. Si des codes de controle se trouvent dans la zone ainsi spécifiée, leurs noms normalisés seront utilisés. Si des octets ne correspondant à aucun de ces cas sont rencontrés dans cette zone, leur valeur précédée du symbole 8 sera automatiquement générée.

- B déclare une zone de constantes organisées en octets. DESASS génère alors des FCB suivis par chaque octet précédé du symbole S. Pour faire un listing présentable, 8 octets au maximum sont générés par FCB et par ligne.

- L déclare une zone de constantes comme étant des valeurs d'étiquettes. DESASS crée alors une zone de FDB considérés comme des étiquettes. Cela est très utile pour désassembler les zones de programmes contenant des tables de sauts ou des tables d'adressage indirect.

- W déclare une zone de constantes organisées en mots de 16 bits. DESASS génère alors des FDB suivis par deux octets (un mot de 16 bits) précédés par le symbole 3.

- R fait une remise à zéro de toutes les zones de constantes précédemment spécifiées. Cette commande est à utiliser lorsque vous avez fait une faute de frappe dans une des spécifications précédentes. Il n'est en effet pas possible de corriger sélectivement tel ou tel type de définition.

- P signale à DESASS que vous avez fini de définir des zones de constantes et qu'il peut donc commencer à travailler.

Les lettres A, B , L et W font demander une adresse de début de zone sous la forme:
Starting address?
Vous devez répondre par l'adresse de début de la zone considérée exprimée en hexadécimal. Une adresse de fin vous est alors demandée sous la forme:
Ending address?
Vous devez répondre l'adresse de fin de la zone considérée exprimée en hexadécimal.
Tant que la lettre P n'a pas été frappée, la ligne "Data Segment Type...." est ré affichée vous permettant de définir autant de zones que vous le désirez.

Si l'option S est spécifiée, DESASS vous demande alors les adresses de début et de fin du segment à désassembler de la façon suivante:
What are the bounds of the segment to disassemble? suivi par les messages Starting Address et Ending Address vus ci avant pour les zones de constantes.

UTILISATION D’UN FICHIER DE COMMANDE

Lors des désassemblages de programmes longs ou complexes, le fait de devoir indiquer les zones de constantes avec l’option B vue ci avant devient très vite pénible. Pour ce faire, il vaut mieux utiliser un fichier de commande qui fera cela tout seul et à votre place. Ce fichier doit etre réalisé par vos soins avec la commande EDIT du DOS en respectant la syntaxe décrite ci apres.

Le fichier de commande est constitué par une suite de lignes, chacune commençant par une commande comprise par le désassembleur. Chaque commande est suivie, sur la même ligne, par les paramètres qu’elle utilise selon les diverses possibilités que voici.

+options permet de spécifier des options avec les mêmes règles que celles vues ci avant dans le chapitre UTILISATION DU DESASSEMBLEUR . Les options D, B, P et S sont, par contre, interdites car pour etre valides elles doivent etre prises en compte avant l’ouverture du fichier de commande ce qui n’est pas le cas si elles sont placées dans ce dernier.

A début-fin permet de spécifier une zone ASCII (voir chapitre précédent). Début et fin sont respectivement les adresses de début et de fin de cette zone exprimées en hexadécimal et séparées l’une de l’autre par un tiret. Ainsi une zone ASCII comprise entre 124 et A02 serait définie par A 124-A02.

B début-fin permet de spécifier une zone de constantes organisées en octets (voir chapitre précédent). Mêmes règles de syntaxe que pour A ci dessus.

L début-fin permet de spécifier une zone de constantes organisées en étiquettes (voir chapitre précédent). Mêmes règles de syntaxe que pour A ci dessus.

W début-fin permet de spécifier une zone de constantes organisées en mots de 16 bits (voir chapitre précédent). Mêmes règles de syntaxe que pour A ci dessus.

S nom de fichier permet de spécifier un nom de fichier contenant des étiquettes qui vous sont propres. Ce fichier doit respecter les règles de syntaxe présentées dans le chapitre suivant. Il est pris par défaut sur le disque de travail et muni de l’extension BIN. Il remplace le fichier standard DISLBL00 ou DISLBL09. Si cette commande S est utilisée seule, aucun fichier d’étiquettes pré définies n’est utilisé.

T nom de fichier permet aussi de spécifier un fichier d’étiquettes comme pour la commande S ci avant. Par contre, il ne vient pas en remplacement de DISLBL00 ou DISLBL09 mais en complément à ce dernier.

Les commandes +, A, B, L et W peuvent intervenir autant de fois que vous le désirez et dans n'importe quel ordre. Les zones de même type n'ont même pas à etre rangées par adresses croissantes, le désassembleur s'en charge. Par contre il ne peut y avoir dans un même fichier de commande qu'une commande T ou une commande S (ou aucune des deux bien sur). En outre, vous pouvez laisser des lignes vides pour clarifier la lecture de votre fichier de commande et même mettre des lignes de commentaires à condition de faire commencer ces_ dernières par une étoile (*) comme .en assembleur. Voici d'ailleurs un exemple de fichier de commande:

```
+Z
*Définition des zones de constantes
B A102-A104
W A105-A108
B 10-15
A A241-A27F
*Utilisation d'un fichier d'étiquettes personnelles
T MESETIQ.BIN
```

Nous y voyons l'option Z qui fait donc désassembler du 6800, suivie d'une ligne de commentaires. Viennent ensuite les différentes zones de constantes dans un ordre quelconque (B 10-15

après B A102-A104). Enfin, une ligne de commentaires précède la

désignation d'un fichier d'étiquettes personnelles qui viendra en complément de DISLBL00.BIN.

LE FICHIER D'ETIQUETTES

Compte tenu du fait que DESASS vous est fourni avec deux fichiers d'étiquettes renfermant toutes les étiquettes standards du DOS 6800 et du DOS 6809 utilisés sur nos divers systèmes, il est peu probable que vous ayez à créer votre propre fichier d'étiquettes. Si tel était le cas, il vous suffirait pour cela de lister DISLBL00.TXT ou DISLBL09.TXT dans lesquels toutes les informations utiles vous sont fournies.
Muni de ces informations, vous pourrez alors créer vos propres fichiers d'étiquettes mais aussi, et c'est peut etre le plus simple, ajouter vos propres étiquettes dans DISLBL00 ou DISLBL09. Dans tous les cas, le fichier d'étiquettes ainsi créé ou modifié doit etre assemblé avec la commande ASMB du DOS pour produire un fichier binaire, seul utilisable par DESASS.

QUELQUES REMARQUES

Comme expliqué en début de manuel, le désassemblage de programmes longs et(ou) complexes nécessite une bonne interaction entre le désassembleur et l'utilisateur et, donc, nécessite un minimum de connaissances en langage d'assemblage 8800 et 6809.

Pour vous faciliter le travail, remarquez que les noms d'étiquettes générés par DESASS (lorsque ce ne sont pas des noms

standards extraits des fichiers d'étiquettes) sont tous de la forme LXXXX où XXXX est l'adresse en hexadécimal à laquelle l'étiquette a été rencontrée. Cela permet très facilement de s'ÿ retrouver au sein d'un programme en cours de désassemblage.

DESASS supporte tous les modes d'adressage du 6809 et génère lorsque c'est nécessaire les symboles > et < de forçage d'adressage 16 bits ou 8 bits (voir si nécessaire la notice de l'assembleur 6809 pour la signification de ces symboles).

Enfin, souvenez vous toujours que tant que vous n'avez rien modifié, tout listing désassemblé par DESASS, même s'il est sans signification suite à de mauvaises définitions des zones de, constantes, peut etre ré assemblé pour donner un programme rigoureusement identique au programme initial.

LES MSSAGES D'ERREURS

DESASS affiche, lorsque c'est nécessaire, des messages d'erreurs. Ces erreurs peuvent avoir deux causes: des erreurs "disques" dues à de mauvaises spécifications de fichiers (erreur de lecteur, mauvais nom de fichier, extension incorrecte) et des erreurs d'utilisation de' _ DESASS lui même (mauvaises spécifications de zones en général). Les messages d'erreurs étant en anglais, nous en donnons ci après la signification pour ceux d'entre vous que la langue de Shakespeare rebute.

Les erreurs disques comportent généralement deux lignes; la première est de la forme:

'Type' File Error où 'Type' peut etre Input, Output, Label ou Command ce qui indique alors- le fichier responsable de l'erreur (Fichier d'entrée, de sortie, d'étiquettes ou de commande). Une deuxième ligne, générée par le DOS celle là, indique le type d'erreur en exploitant les messages de ERREURS.SÏS ou les numéros de codes d'erreurs du DOS standard si ERREURS.SYS n'est pas présent sur votre disque système.

Les erreurs d'utilisation de DESASS sont en général dues à des lignes du fichier de commande; en effet, en mode interactif, ces dernières sont immédiatement détectées et les questions nécessaires sont posées à nouveau. En général, le numéro de ligne du fichier de commande ayant causé l'erreur est affiché sous la forme:

Command file line #NNNN où NNNN est le numéro de ligne en question.

Les erreurs ainsi reconnues peuvent etre les suivantes:

- Syntax error in command line qui correspond à une erreur de syntaxe dans la ligne d'appel de DESASS.

- Start > End, Reenter both addresses qui signale une adresse de

début supérieure à une adresse de fin et qui demande de frapper à nouveau les deux adresses.

- Illesal entrÿ, re-enter qui indique qu'un nombre hexadécimal incorrect a été frappé et qui le demande à nouveau.
- Command syntax error qui indique qu'une ligne du fichier de commande est incompréhensible pour DESASS.

- Illegal segment address specification qui indique qu'une spécification d'adresse d'un segment à désassembler est incorrecte.

- Multiple S or T command in command file qui indique qu'il y a plus d'une commande S ou T dans le fichier de commande.

- Illégal option switch qui indique un choix d'option incorrect.

- Word or Label segment has odd length qui indique qu'une zone de constantes d'adresses ou de mots de 16 bits contient un nombre d'octets impair ce qui est impossible puisqu'une telle zone ne contient que des mots de 16 bits (et donc des paires d'octets).

– Data segment overlap qui indique que des zones de constantes se recouvrent ce qui n'est pas admis.

- Tables out of memorÿ qui indique que la mémoire disponible sur le sytème est insuffisante pour contenir toutes les tables nécessaires au désassemblage (exceptionnel).

UTILISATION D'UNE IMPRIMANTE

Comme toutes lest commandes du DOS, DESASS peut etre précédé de la commande P afin de pouvoir utiliser une imprimante. Cette façon de faire n'est toutefois pas recommandée car elle est assez peu pratique et ne présente pas d'intéret. Il est de loin préférable de créer un fichier disque du programme à désassembler

et de faire lister ensuite ce dernier par un P LIST lorsque le désassemblage est au point et terminé.