

Расширенный экранный отладчик XDBG для MSX

Автор: Леонид Бараз

В тексте данного документа применяются следующие обозначения для клавиш: пробелом разделяются клавиши, которые нужно нажимать последовательно, а плюсом — одновременно.

Руководство пользователя

Программа XDBG представляет собой экранный отладчик программ, написанных на ассемблере Z80. Этот отладчик может использоваться на ПЭВМ [MSX 2](#) и [MSX](#), оснащенных [Yamaha V9938 \(VDP\)](#) ([Yamaha YIS-503IIR](#)), под управлением операционной системы [dos](#) (в том числе в варианте Ю.В.Галутина). Также работает под [MSX-DOS 2](#) и [Nextor](#).

Команда вызова отладчика:

```
XDbg[/p[/s]][/M] [имя-программы]
```

После XDbg в команде запуска можно указать от одного до трех флажков, которые определяют, в каком слоте памяти должен располагаться собственно отладчик. Первые два флажка определяют номера первичного и вторичного слота соответственно XDbg/3/0 — слот 3-0, XDbg/1 — слот 1 нерасширенный). Флажок /M предписывает использование маппера (отладчик располагается в страницах FF, FE и FD). При переносе отладчика максимально возможный размер загружаемой и отлаживаемой программы может достигать 48Кбайт.

При отсутствии флажков отладчик размещается в основной оперативной памяти, оставляя для программы пользователя вместе с таблицей символических имен только 32Кбайт. Однако перенести отладчик в параллельную память можно и в процессе работы посредством команды `ESC U` (см. ниже).

Примеры отображения на экране:

Режим листинга ассемблера

окно заголовка

02000	List	X-DEBUGGER Version 1.0	Help:<Esc>?	Visual:Trace	EI PC=D827 I=00 8B/02/8B/8B R=58 --/--/--/-- T=838B:CE6B/89C3
00~00		7FF8:60 LD H,B 7FF9:4B LD C,E 7FFA:03 INC BC 7FFB:1A LD A,(DE) 7FFC:FE 38 CP 38 7FFE:FF RST 38 7FFF:FF RST 38			A=00 . sZxHxpNC BC=0240: 00 . DE=0000: C3 "ц" HL=7FFD: 38 "8" IX=1377: 2A "*" IY=0A00: 53 "S"
C0-C0		MEM80@:8000:00 NOP 8001:00 NOP 8002:00 NOP		0078	
20+1A		8003:20 FB JR NZ,MEM80@:8000 8005:DD 2A 08 80 LD IX,(PRED:8008)			A'=00 . szxhxpnc BC'=0120: E1 "A" DE'=0A00: 53 "S" HL'=1100: 0E .
00+00		8009:C1 POP BC 800A:CD CD D9 CALL D9CD			
-		3FC0:E7 38 EB 2A E9 38 7D 93 6F 7C 9A 67 22 EB 38 2A 3FD0:E7 38 EB 21 18 39 C3 0A 1F CD 36 11 22 E9 38 EB 3FE0:2A E7 38 7B 95 6F 7A 9C 67 22 EB 38 2A E9 38 EB 3FF0:21 1E 39 C3 0A 1F 0E 07 25 3D 20 03 E9 3C 32 03			Г8K*I8}.o .g"K8* Г8K!.9ц..м6."И8K *Г8{.oz.g"K8*I8K !.9ц....%=.И<2.
+	DRIVER:	4000:41 42 6F 57 76 65 00 00 00 00 00 00 00 00 00 00 4010:C3 F5 74 C3 86 78 C3 09 79 C3 23 79 C3 50 79 C3 4020:82 78 C3 35 5B 37 C3 AC 60 C3 14 62 00 C3 AE 5F			ABowVe..... цYтц.хц.уц#уцPyц .хц5[7ц∞`ц.b.ц€_
~					

Режим загрузки программы

окно запроса (дополнительное окно файлов)	
1F000	
Input	File:B:prog .COM Area:07F0-BEFC Reloc:0100->07F0
	EI PC=0100 I=00 8B/8B/8B/8B R=7B FB/FA/F9/F8 T=BEFB:CE6B/89C3
	012F:CB 16 RL (HL) 0131:30 0F JR NC,0142 0133:E5 PUSH HL 0134:DD 66 00 LD H,(IX+00) 0137:DD 6E FF LD L,(IX-01) 013A:19 ADD HL,DE 013B:DD 74 00 LD (IX+00),H 013E:DD 75 FF LD (IX-01),L 0141:E1 POP HL 0142:DD 23 INC IX 0144:0B DEC BC 0145:78 LD A,B 0146:B1 OR C 0147:20 DF JR NZ,0128
	A=00 . szxhxpnc BC=0000: C3 "ц" DE=0000: C3 "ц" HL=0000: C3 "ц" IX=0000: C3 "ц" IY=0000: C3 "ц"
	A'=00 . szxhxpnc BC'=0000: C3 "ц" DE'=0000: C3 "ц" HL'=0000: C3 "ц"
V	1F020:17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
V	1F030:17 17 17 17 17 17 17 17 17 17 17 17 17 17 12 17
V	1F040:17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 19
V	1F050:16 49 6E 70 75 74 16 20 46 69 6C 65 3A 20 70 72 .Input. File:B:P
V	1F060:6F 67 20 20 20 20 20 20 20 20 41 72 65 61 3A 20 ROG .COM Are
V	1F070:30 37 46 30 2D 38 41 31 42 20 20 52 65 6C 6F 63 a:07F0-8A1B Rel
V	1F080:3A 20 30 31 30 30 2D 3E 30 37 46 30 20 20 16 20 oc:0100->07F0 .
V	1F090:45 49 20 50 43 3D 30 31 30 30 20 52 3D 37 42 16 EI PC=0100 .

Отладчик обеспечивает:

- загрузку в память и запись на диск программ и таблиц символов (файлов <имя>.<тип> и <имя>.SYM);
- просмотр и корректировку содержимого оперативной памяти в символьном и шестнадцатиричном формате, а также в виде команд ассемблера;
- просмотр и корректировку содержимого видеопамати в символьном и шестнадцатиричном формате;
- просмотр и изменение содержимого регистров отлаживаемой программы;
- использование имен, введенных вместе с программой, а также добавление новых имен и удаление имеющихся (имена используются и в командах ассемблера); имена можно настроить на начальный адрес программы;
- выдачу на печать содержимого текущего окна отладчика;
- установку и снятие точек приостанова (со счетчиками);
- установку и снятие контроля изменения байтов памяти;
- покомандное и непрерывное выполнение программы (в том числе и в режиме мультипликации, с обходом и без обхода команд **CALL**);
- возврат управления отладчику: при достижении точки приостанова с нулевым счетчиком, при изменении одного из контролируемых байтов памяти, при нормальном завершении программы, при нажатии клавиши **STOP**;
- пересылку и заполнение областей памяти, поиск символьного или шестнадцатиричного образца.
- выполнение арифметических действий над шестнадцатиричными числами;
- получение на экране краткой информации о средствах, имеющихся в отладчике.

При запуске отладчик переводит систему в 80-символьный режим и загружает в оперативную память программу, если ее имя указано в команде (имя указывается без уточнения; загружаются файлы <имя>.<тип> и <имя>.SYM).

В процессе работы на экране выделяются поля разметки и поля данных. Курсор всегда находится в одном из полей данных, и только в такие поля можно вносить изменения. При выходе курсора из текущего поля его новое

содержимое проверяется и заносится в память машины; все остальные поля экрана при этом приводятся (по возможности) в соответствие с содержимым изменённого поля. Например, для изменения байта или слова данных в любом поле достаточно просто набрать его новое значение и выйти из поля. Аналогично, для того, чтобы передвинуть окно листинга или дампа на другие адреса памяти, достаточно в любой строке набрать нужное имя в поле имени или нужный адрес в поле адреса. Для создания нового имени достаточно набрать его в соответствующем поле, а для удаления существующего — заменить его на новое или заполнить поле имени пробелами.

Все поля данных, имеющиеся на экране, сгруппированы в окна: три основных («дампа», «листинга» и «регистров») и одно дополнительное («заголовка», «файлов» или «памяти»). Курсор перемещается в пределах одного окна с помощью стрелок, клавиш **Ввод**, **TAB** и **Ctrl+F**. Листание осуществляется по клавишам **Ctrl+J** (вверх) и **Ctrl+Q** (вниз). Редактирование информации выполняется символьными клавишами, а также клавишами **INS**, **DEL** и **BS**. Переход в другое окно (и установка дополнительного окна) выполняются по одной из следующих команд:

1. **ESC L** Работа в окне листинга ассемблера.

Левая колонка содержит точки приостанова (для них указывается максимальный счетчик, признак активности:

- + - активна,
- ~ - активна в параллельном банке памяти,
- - - неактивна

и текущее значение счетчика. В основной части каждой строки окна располагаются поля имени, адреса, байтов, образующих команду, и самого текста команды.

Правая колонка окна содержит значения счетчиков профилей выполнения программы (в строках команд с символическими именами).

Имена во всех полях (в том числе и в текстах команд) должны заканчиваться двоеточием. Например, команды могут записываться в следующем виде:

```
LD    A, (name:3000)
LD    A, (name: )
LD    A, (3000)
```

Команда **RST 30** (Inter-Slot Call) дополняется в качестве операндов номером слота и адресом вызова.

2. **ESC D** Работа в окне дампа.

Левая колонка содержит признаки контроля изменения байта памяти с указанием активности контроля (+/-/~). В основной части каждой строки окна имеются поля имени, адреса, 16 полей байтов в шестнадцатичном виде и 16 полей тех же байтов в символьном виде.

3. **ESC V** Работа в окне дампа видеопамати.

Содержимое видеопамати отображается так же, как и в режиме **ESC D**, однако левая колонка заполняется буквами **V** (для VRAM) или **E** (для ERAM). При просмотре VRAM поле адреса дополняется слева еще одним разрядом, чтобы охватить все 128 Кбайт.

4. **ESC R** Работа в окне регистров.

Окно содержит поля значений всех регистров, а также байтов или слов, на которые указывают шестнадцатититные регистры. Одновременно с шестнадцатичными значениями байтов выдается их символьное представление.

Кроме того, имеются поля счетчика команд (PC), состояния обработки прерывания (EI/DI) и выбранного банка памяти (с указанием слота и страницы маппера) для всех четырех 16 Кбайтных страниц. Наличие или отсутствие маппера распознается автоматически.

5. **ESC Y** Показ символических имен.

Окно листинга ассемблера заполняется строками, соответствующими символическим именам.

6. **ESC B** Показ точек приостанова.

Окно листинга ассемблера заполняется строками, соответствующими точкам приостанова.

7. **ESC H** Показ контролируемых байтов.

Окно дампа заполняется строками, соответствующими адресам байтов, изменение которых контролируется.

8. **ESC I** Чтение файлов.

В дополнительном окне располагаются поля имени файла и интервала адресов для размещения программы. После нажатия клавиши перевода строки файл с именем <имя>.<тип> считывается в память (конфигурация слотов и маппера определяется соответствующими полями в окне регистров).

Кроме того, к таблице имен присоединяются имена из файла <имя>.SYM, если он есть. С помощью полей Reloc: можно указать настройку символических имен на нестандартный начальный адрес программы.

9. **ESC O** Запись файлов.

В дополнительном окне располагаются поля имени файла и интервала адресов. После нажатия клавиши перевода строки указанная область памяти записывается в файл <имя>.<тип>, а все символические имена — в файл <имя>.SYM (конфигурация слотов и маппера определяется соответствующими полями в окне регистров).

10. **ESC P** Выдача на печать содержимого текущего окна отладчика (печать прерывается при нажатии **CTRL+STOP**).

11. **ESC M** Пересылка информации.

В дополнительном окне располагаются поля запроса двух интервалов адресов: откуда и куда требуется переслать информацию. При изменении начального адреса в одном из интервалов соответствующий конечный адрес автоматически изменяется так, чтобы длины интервалов совпали. При изменении конечного адреса таким же образом меняется конечный адрес другого интервала.

12. **ESC F** Заполнение области памяти.

В дополнительном окне располагаются поля запроса интервала адресов и образца для заполнения. Образец для заполнения может быть набран в символьном или шестнадцатиричном виде (вид определяется полем, содержащим букву С или Х соответственно). Размер образца определяется положением курсора в момент нажатия клавиши **Ввод**.

13. **ESC S** Поиск образца.

В дополнительном окне располагаются поля запроса интервала адресов и образца для поиска. Образец для поиска может быть набран в символьном или шестнадцатиричном виде (вид определяется полем, содержащим букву С или Х соответственно). Размер образца определяется положением курсора в момент нажатия клавиши <перевод строки>. Поиск можно прервать нажатием **CTRL+STOP**.

14. **ESC E** Начальная установка регистров.

Все регистры устанавливаются в 0, счетчик команд PC устанавливается на 100h, состояние прерываний — разрешены (EI), всем страницам памяти сопоставлены основные банки памяти (установленные при запуске отладчика).

15. **ESC Z** Начальная установка текущих счетчиков точек приостанова (они устанавливаются равными максимальным счетчикам).

16. **ESC C** Шестнадцатиричный калькулятор.

В дополнительном окне располагаются два поля операндов (четырёхзначные шестнадцатиричные числа), поле знака операции (+, -, *, /, %) и поле показа результата. Поле результата заполняется при смене любого операнда или знака операции.

17. **ESC T** Установка базового адреса PNT и PGT отладчика.

Поле базового адреса располагается в левом верхнем углу рамки. При вводе нового значения в этом поле PNT и PGT переносятся на указанный адрес и автоматически инициализируются. Таблицы PNT и PGT занимают 1000h байт VRAM, начиная с указанного адреса.

18. **ESC U** Перенос отладчика в параллельную память.

Программы и данные самого отладчика переносятся в ту память, которая задана полями слотов и маппера в окне регистров. При этом для загрузки и отладки программ пользователя становится доступным около 48 Кбайт памяти.

Перенос в параллельную память не может быть выполнен, если хотя бы одна из трех страниц (0000-3FFF, 4000-7FFF, 8000-BFFF) совпадает с первоначальной по слотовому адресу. Кроме того, если при запуске отладчика или в процессе работы перенос выполнен, его нельзя ни отменить, ни изменить; можно только выйти из отладчика и загрузить его снова.

19. **ESC Q** Завершение работы отладчика и выход в среду операционной системы с восстановлением исходного режима экрана (40/80 символов).
20. **ESC ?** Показ страницы с подсказкой.
21. **CTRL+G** Запуск программы.

Программа начинает выполняться с адреса, находящегося в счетчике команд PC. Устанавливается заданное пользователем распределение банков памяти. Если режим мультипликации выключен (Visual:No), на время работы программы экран переключается на обычную страницу системы (0000h). Если же режим мультипликации включен (Visual:Exeс или Trace), системная страница не включается, зато после каждой исполненной команды обновляется содержимое экрана отладчика. В режиме Visual:Exeс исполняется отдельно каждая команда, а в режиме Visual:Trace взамен одной команды **CALL** исполняется вся вызываемая подпрограмма.

Все точки приостанова устанавливаются в основных банках памяти (которые были включены при запуске отладчика).

При достижении одной из активных точек приостанова (с признаком «+» или «~») либо выполняется уменьшение счетчика (если он ненулевой), либо приостанавливается выполнение программы и управление передается отладчику. Аналогично выполнение программы приостанавливается при изменении содержимого одного из активных контролируемых байтов. Следует иметь в виду, что выполнение программы значительно замедляется при установке контроля изменения байтов.

Выполнение программы можно приостановить нажатием клавиши **STOP** (если прерывания в этот момент разрешены). При выполнении команды RET с начальным состоянием стека или команды RST 0 управление также передается отладчику; при этом считается, что программа успешно завершена.

Обработка точек приостанова организуется с помощью RST 0, поэтому все остальные команды RST могут использоваться в отлаживаемой программе без ограничений. После возврата управления отладчику в окне листинга ассемблера первая строка устанавливается на команду, с которой начиналось выполнение, а вторая — на ту, которая вызвала приостанов (в ней устанавливается курсор).

Передача управления отладчику при достижении точки приостанова или при завершении программы возможна только при условии, что странице 0000h-3FFFh в этот момент сопоставлен основной банк памяти (тот же, что и при запуске отладчика).

При выполнении программы ведется подсчет профилей по всем символическим именам (при каждом прерывании и при трассировке отдельной команды увеличивается на единицу счетчик профиля ближайшего символического имени с адресом, меньшим текущего PC). Значения счетчиков профиля отображаются в правой колонке окна листинга ассемблера.

22. **CTRL+X SELECT** Выполнение одной команды.

Выполняются те же действия, что и по указанию **CTRL+G**, но исполняется только одна команда (расположенная по адресу из счетчика команд PC). Можно исполнять также команды, находящиеся в ПЗУ (однако точки приостанова в ПЗУ устанавливать нельзя).

23. **CTRL+T** Выполнение команды с обходом подпрограммы.

Выполняется аналогично **CTRL+X**, но для команды **CALL** управление возвращается отладчику только после выполнения вызываемой подпрограммы. При выполнении подпрограммы выполняется обычная обработка точек приостанова (как в **CTRL+G**).

24. **CTRL+p** Установка счетчика команд PC на ту команду, против которой находится курсор.

25. **CTRL+V** Выбор режима мультипликации.

Устанавливается один из режимов Visual:No, Exeс или Trace.

Распределение видеопамати:

0000h	PNT системы и программы
1000h	PGT системы и программы
2000h	PNT отладчика
2800h	PGT отладчика
3000h	PNT подсказки

[dbgrdv.zip](#), оригинал

Ссылки

<http://fms.komkon.org/MSX/DBGRDV.zip>

<http://sysadminmosaic.ru/msx/xdbg/xdbg?rev=1593454995>

2020-06-29 21:23

