Машинно-зависимые языки программирования, лекция 7

Каф. ИУ7 МГТУ им. Н. Э. Баумана, 2022 г.

Макроопределения

Макроопределение (макрос) - именованный участок программы, который ассемблируется каждый раз, когда его имя встречается в тексте программы.

- Определение:
  имя MACRO параметры
  ……
  ENDM
- Пример:
  load_reg MACRO register1, register2
  push register1
  pop register2
  ENDM

Директива присваивания =

Директива присваивания служит для создания целочисленной макропеременной или изменения её значения и имеет формат:
Макроимя = Макровыражение

- Макровыражение (или Константное выражение) - выражение, вычисляемое препроцессором, которое может включать целочисленные константы, макроимена, вызовы макрофункций, знаки операций и круглые скобки, результатом вычисления которого является целое число
- Операции: арифметические (+, -, *, /. MOD), логические, сдвигов, отношения

Директивы отождествления EQU, TEXTEQU

Директива для представления текста и чисел:

Макроимя EQU нечисловой текст и не макроимя ЛИБО число

Макроимя EQU <Операнд>

Макроимя TEXTEQU Операнд

- Пример:

  X EQU [EBP+8]

  MOV ESI,X

Макрооперации

- % - вычисление выражение перед представлением числа в символьной
- форме
- <> - подстановка текста без изменений
- & - склейка текста
- ! - считать следующий символ текстом, а не знаком операции
- ;; - исключение строки из макроса

Блоки повторения

- REPT число … ENDM - повтор фиксированное число раз
- IRP или FOR:
  IRP form,<fact_1[,fact_2,...]> … ENDM
  Подстановка фактических параметров по списку на место формального
- IRPC или FORC:
  IRPC form,fact … ENDM
  Подстановка символов строки на место формального параметра
- WHILE:
  WHILE cond … ENDM

Директивы условного ассемблирования

- IF:
  IF c1
  ...
  ELSEIF c2
  ...
  ELSE
  ...
  ENDIF
- IFB <par> - истинно, если параметр не определён
- IFNB <par> - истинно, если параметр определён
- IFIDN <s1>,<s2> - истинно, если строки совпадают
- IFDIF <s1>,<s2> - истинно, если строки разные
- IFDEF/IFNDEF <name> - истинно, если имя объявлено/не объявлено

Директивы управления листингом

- Листинг - файл, формируемый компилятором и содержащий текст ассемблерной программы, список определённых меток, перекрёстных ссылок и сегментов.
- TITLE, SUBTTL - заголовок, подзаголовок на каждой странице
- PAGE высота, ширина
- NAME - имя программы
- .LALL - включение полных макрорасширений, кроме ;;
- .XALL - по умолчанию
- .SALL - не выводить тексты макрорасширений
- .NOLIST - прекратить вывод листинга

Комментарии

comment @

... многострочный текст...

@

Виды трансляторов ассемблера

- MASM
- TASM
- NASM
- FASM
- YASM
- as
- ...

AT&T-синтаксис

Синтаксис стандартного ассемблера для UNIX - **as**

Основные отличия от Intel-синтаксиса:

1. Имена регистров предваряются префиксом %.
2. Обратный порядок операндов: вначале источник, затем приёмник.
3. Размер операнда задается суффиксом, замыкающим инструкцию.
4. Числовые константы записываются в Си-соглашении.
5. Для получения смещения метки используется префикс $.

Создание оконных приложений на ассемблере под x86

Системный вызов — обращение прикладной программы к ядру операционной системы для выполнения какой-либо операции.

Для реализации оконных приложений необходима линковка с соответствующими библиотеками и использование как их функций, так и системных вызовов.

Дизассемблирование. Реверс-инжиниринг

Дизассемблер - транслятор, преобразующий машинный код, объектный файл или библиотечные модули в текст программы на языке ассемблера.

Дизассемблирование - процесс получения текста программы на ассемблере из программы в машинных кодах.

Реверс-инжиниринг (обратная разработка) — исследование готовой программы с целью понять принцип работы, поиска недокументированных возможностей или внесения изменений.