Assembly language programming
By xorpd

BASIC ASSEMBLY

Addressing rules of thumb

xorpd.net

Objectives

- We will study some rules of thumb to verify our address calculations.

Understanding addressing

- Addressing can become tricky.

- Example:
  - `add dl,byte [esi + edi]`
    - What is esi, and what is edi?

Years

- Let’s consider years first.
- Let’s look at the two years 1992 and 2014.
  - It doesn’t make sense to add those two numbers.
  - We could subtract them though, and get a meaningful result.
    - The amount of years that has passed between 1992 and 2014.
- We could add 5 years to the year 2014, to get the year 2019.

Years (Cont.)

- We make the following distinction:
  - There are “years”, and there are “intervals”.
  - Years are **big** numbers. (Generally)
  - Intervals are **small** numbers.

- Examples:
  - The year 1992 is of type “year”.
  - The quantity 5 years is of type “interval”.

- Arithmetic:
  - year + interval = year [1995 + 6 = 2001]
  - interval + interval = interval [3 + 5 = 8]
  - year + year is meaningless. [1992 + 2014 is meaningless]
  - year – year = interval. [2012 – 2005 = 7]

Addressing

- Address arithmetic:
  - We distinct between **big** numbers and **small** numbers.
    - Addresses are **big** numbers.
    - Offsets are **small** numbers.

- Address arithmetic rules of thumb:
  - big + small = big
  - small + small = small
  - big + big is meaningless.
  - big – big = small.

Example (1)

```
struct PNT
    x dd ?
    y dd ?
ends

section '.data' data readable writeable
           ; Declare a point:
           my_pnt     PNT        3,4

section '.text' code readable executable
start:
           mov        eax,dword [my_pnt + PNT.y]
           call       print_eax
```

- my_pnt is a “big number”. (Address)
- PNT.y is a “small number”. (offset)
- my_pnt + PNT.y is a “big number”. (Address)
- my_pnt + my_pnt is meaningless.

Example (2)

- `add dl,byte [esi + edi]`
  - esi + edi is an address (A big number).
  - Hence one of esi, edi must be a big number, and the other number must be a small number.
    - We could find out which is which from the rest of the code.
  - It can’t be that both esi and edi are addresses. (big+ big is meaningless)
  - It can’t be that both esi and edi are small numbers (small + small = small).

Summary

- Use the rules of thumb to verify your address arithmetic:
  - big + small = big
  - small + small = small
  - big + big is meaningless.
  - big – big = small.
- For every number related to addressing, ask yourself:
  - Is this a **big** or a **small** number?
- Remember that these are just rules of thumb.