© 2013 МГУ/ВМК/СП

Лекция 3

16 февраля

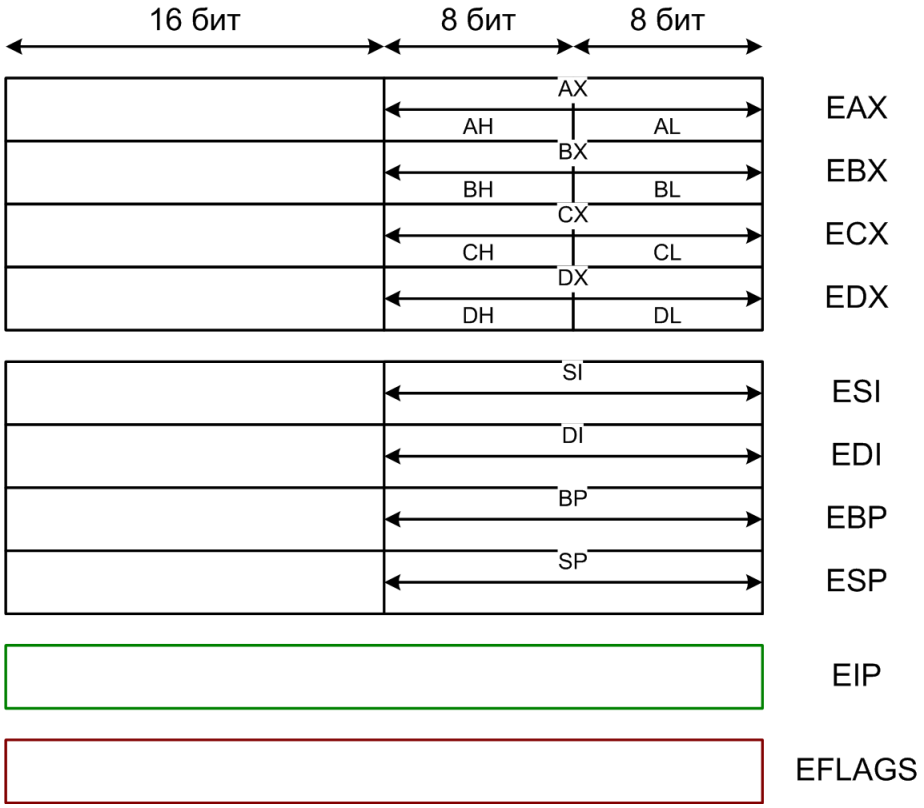
© 2013 МГУ/ВМК/СП

```
%include 'io.inc'

section .data
 a    dw 1
 addr dd $
 var  dd 0x1234F00D

section .bss
   cntr resd 1

section .text
global CMAIN
CMAIN:
   add dword [cntr], 1
   mov eax, [addr]
   PRINT_HEX 4, eax
   NEWLINE
   PRINT_HEX 4, addr
   NEWLINE
   xor eax, eax
```

© 2013 МГУ/ВМК/СП

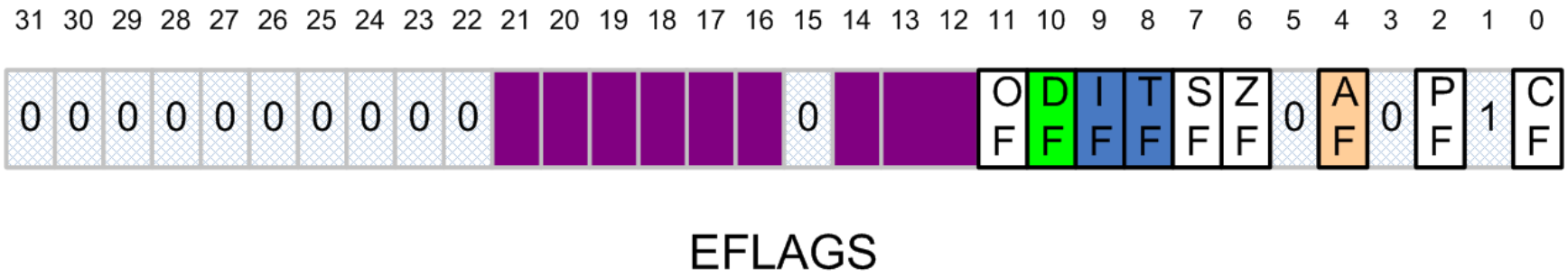
Основные арифметические команды

- MOV
- MOVSX, MOVZX
- ADD, SUB
- NEG
  - r/m 8/16/32
- MUL
  - r/m 8/16/32
- IMUL
  - r/m 8/16/32
  - r 16/32, r/m 16/32
  - r 16/32, r/m 16/32, imm 16/32
- DIV, IDIV
  - r/m 8/16/32
- CBW, CWD, CDQ



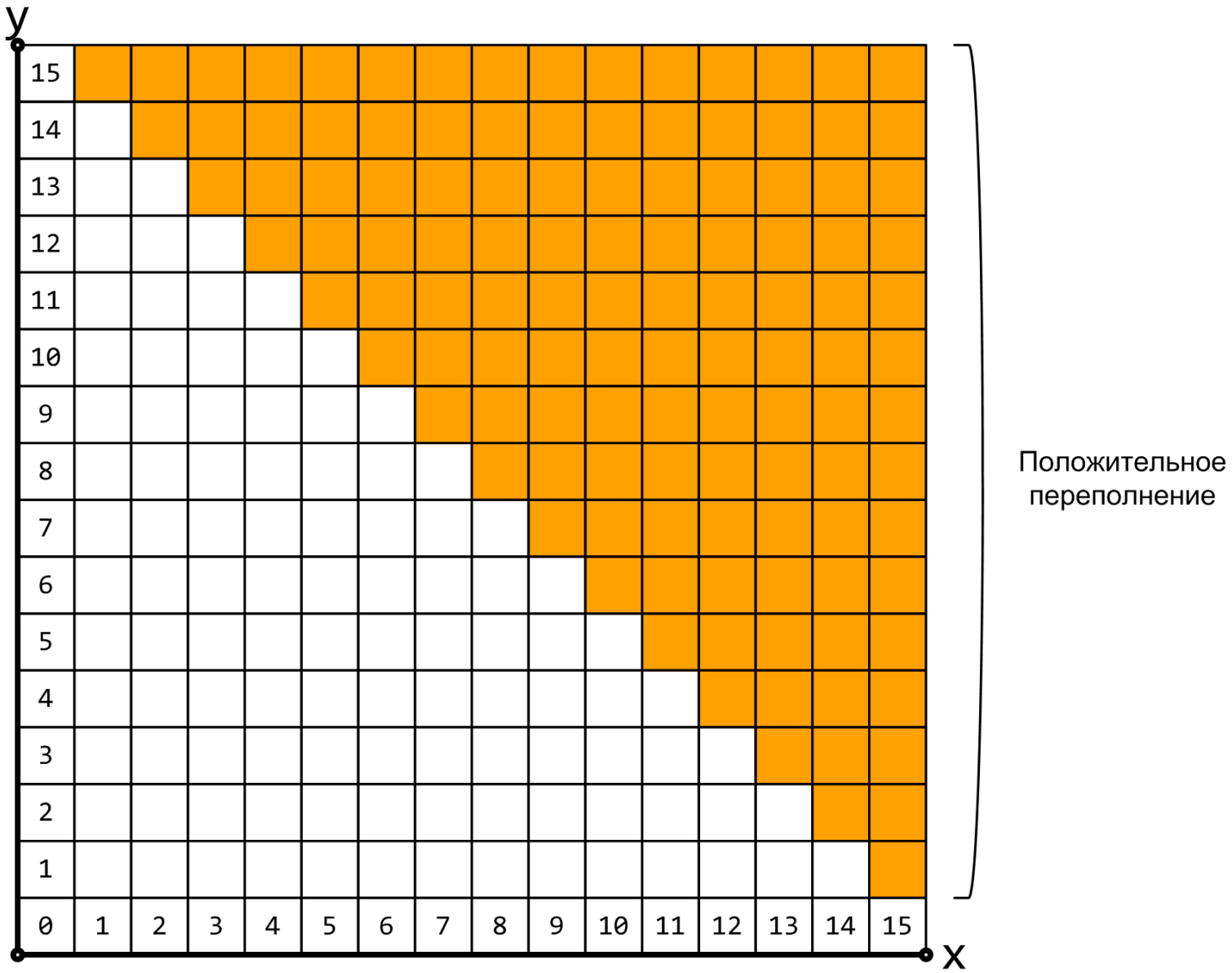
© 2013 МГУ/ВМК/СП

Регистр EFLAGS

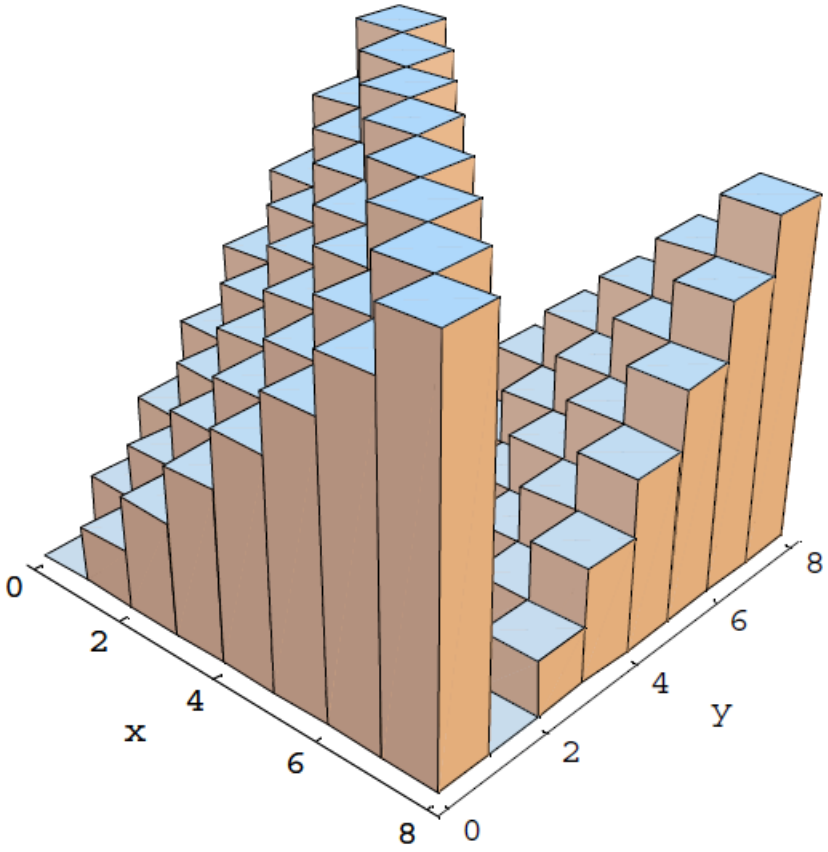


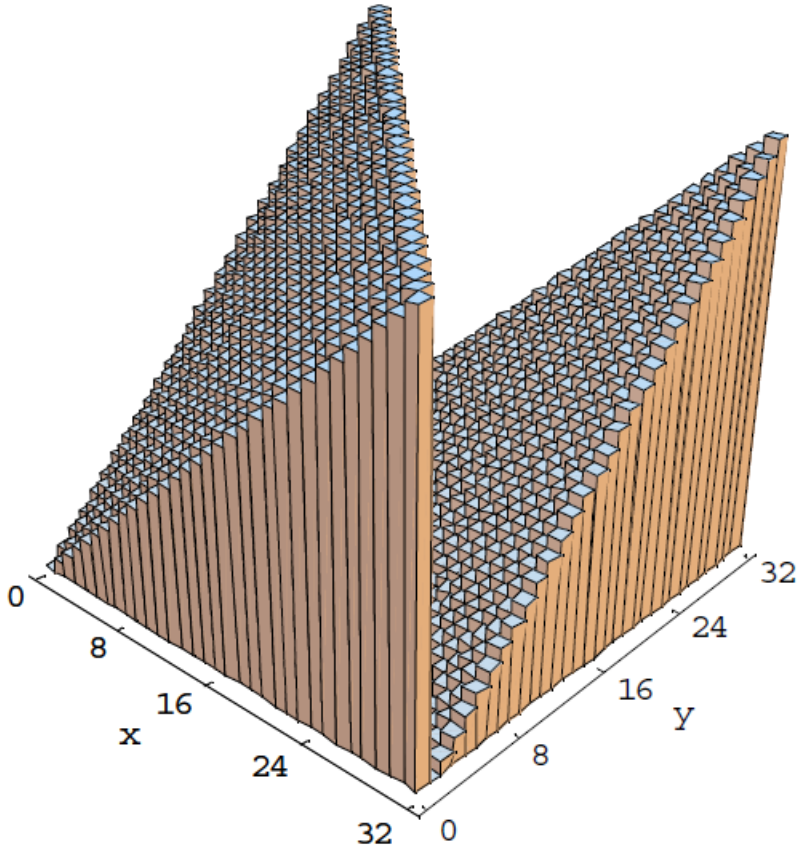
EFLAGS

© 2013 МГУ/ВМК/СП



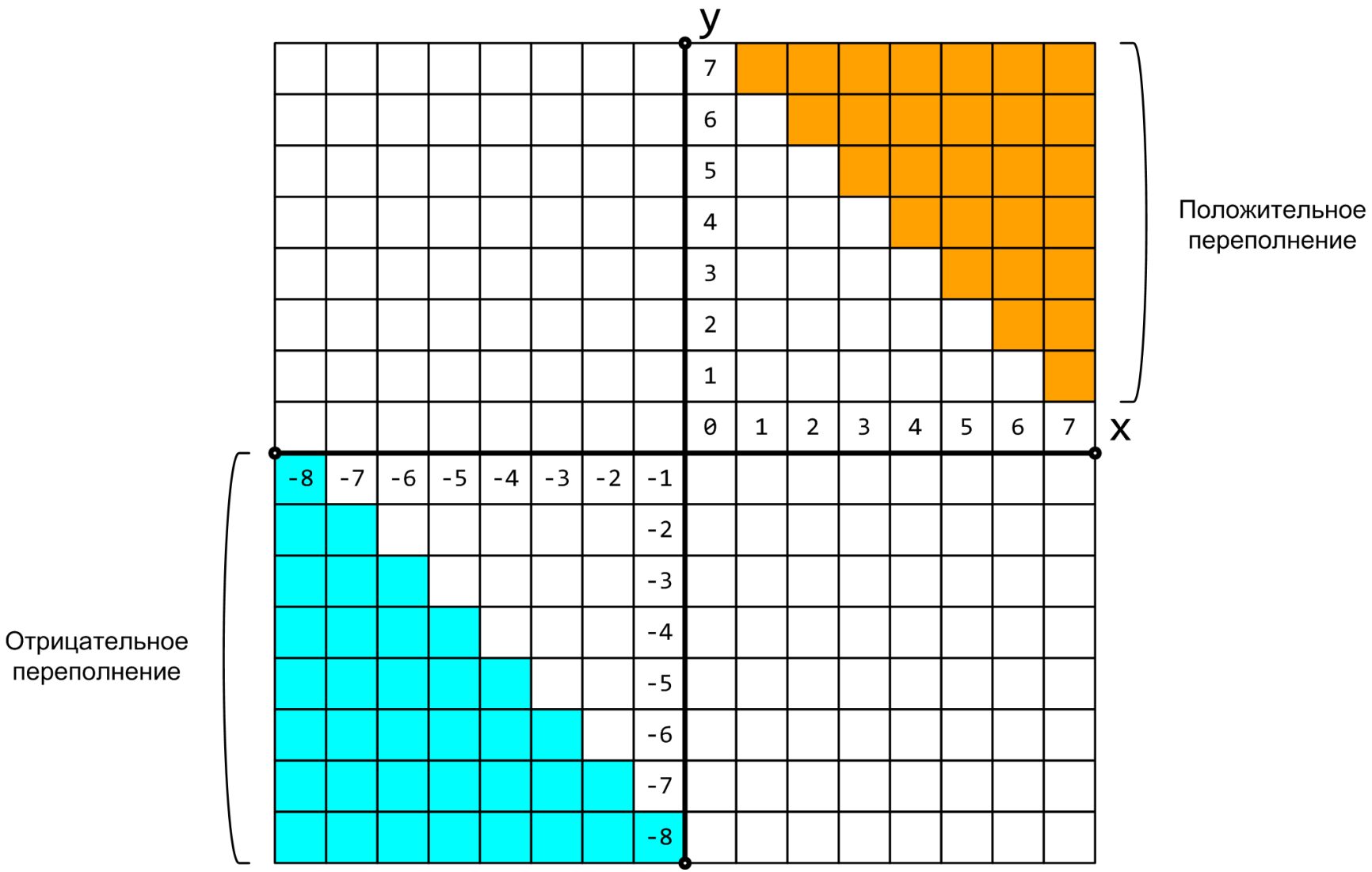
© 2013 МГУ/ВМК/СП





http://www.hackersdelight.org/plotsAdd.pdf

© 2013 МГУ/ВМК/СП



© 2013 МГУ/ВМК/СП

Естественный порядок выполнения

EIP	Машинный код	Длина	Ассемблерная инструкция
8048345	89 e5	2	mov ebp,esp
8048347	83 ec 10	3	sub esp,0x10
804834a	c7 45 f0 02 00 00 00	7	mov dword [ebp-16],0x2

Прибавляем к значению регистра EIP длину в байтах декодированной команды

© 2013 МГУ/ВМК/СП

Изменение естественного порядка выполнения программы

- Арифметические операции
- CMP
  - r/m 8/16/32, imm 8/16/32
  - r/m 8/16/32, r 8/16/32
  - r 8/16/32, r/m 8/16/32
- TEST
  - r/m 8/16/32, imm 8/16/32
  - r/m 8/16/32, r 8/16/32
- JMP
  - r/m/imm 32
- Jcc
  - imm32
- Переходы
  - Абсолютные
  - Относительные