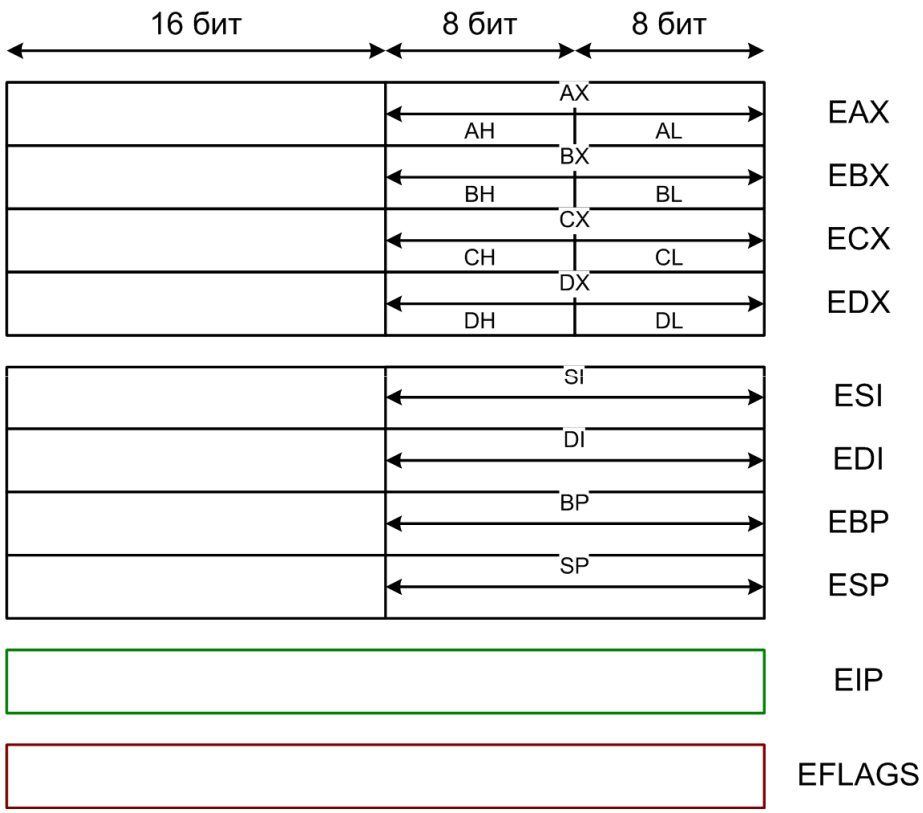
Лекция 3

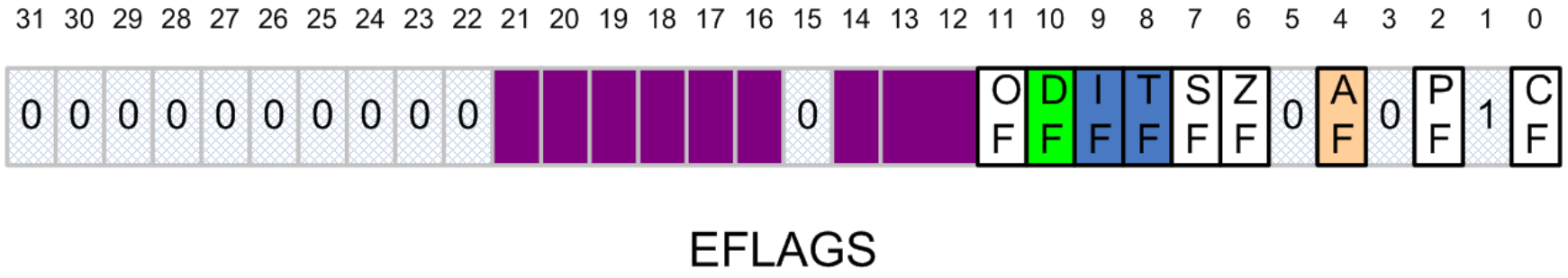
15 февраля

Основные арифметические команды

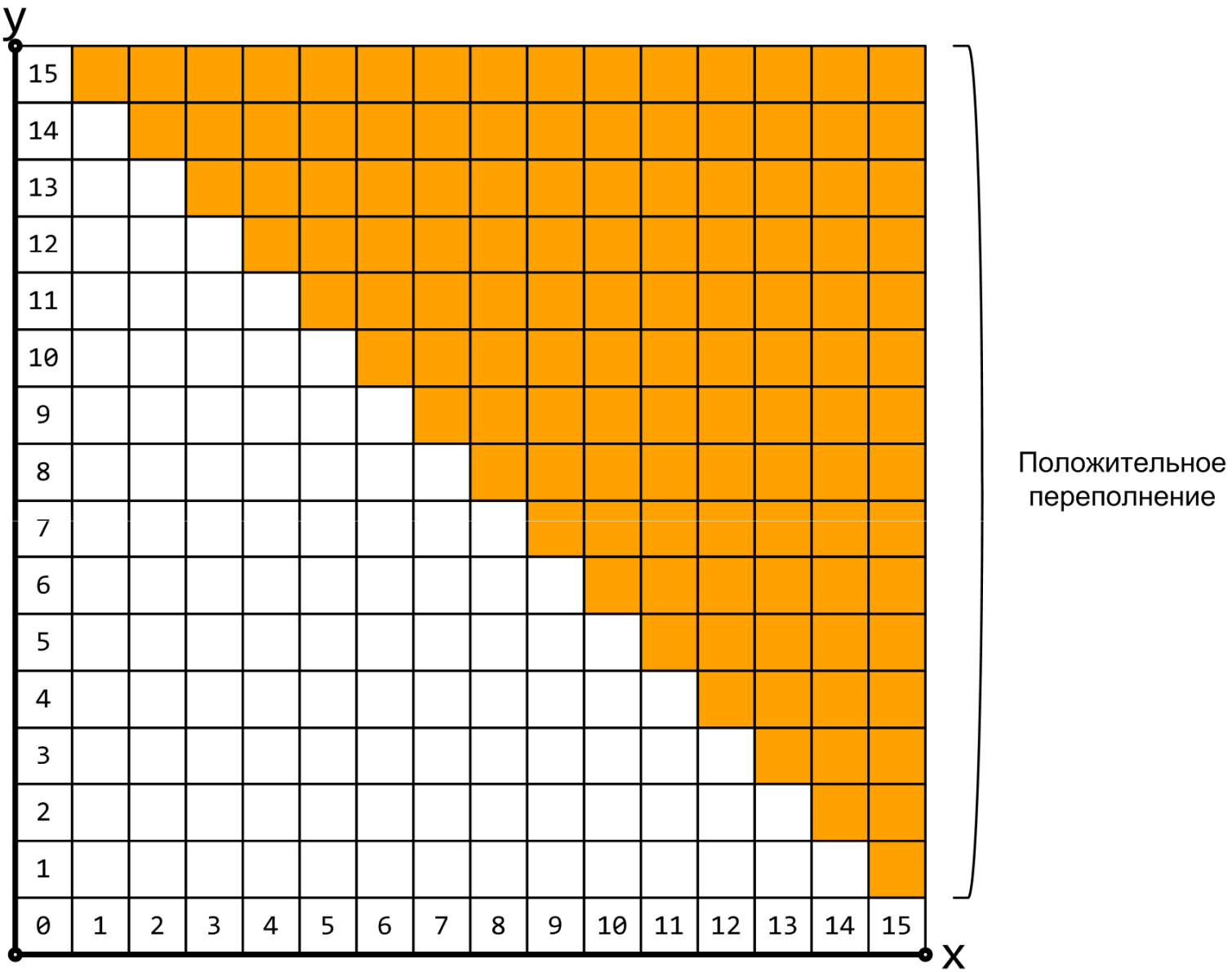
- MOV
- MOVSX, MOVZX
- ADD, SUB
- NEG
  - r/m 8/16/32
- MUL
  - r/m 8/16/32
- IMUL
  - r/m 8/16/32
  - r 16/32, r/m 16/32
  - r 16/32, r/m 16/32, imm 16/32
- DIV, IDIV
  - r/m 8/16/32
- CBW, CWD, CDQ

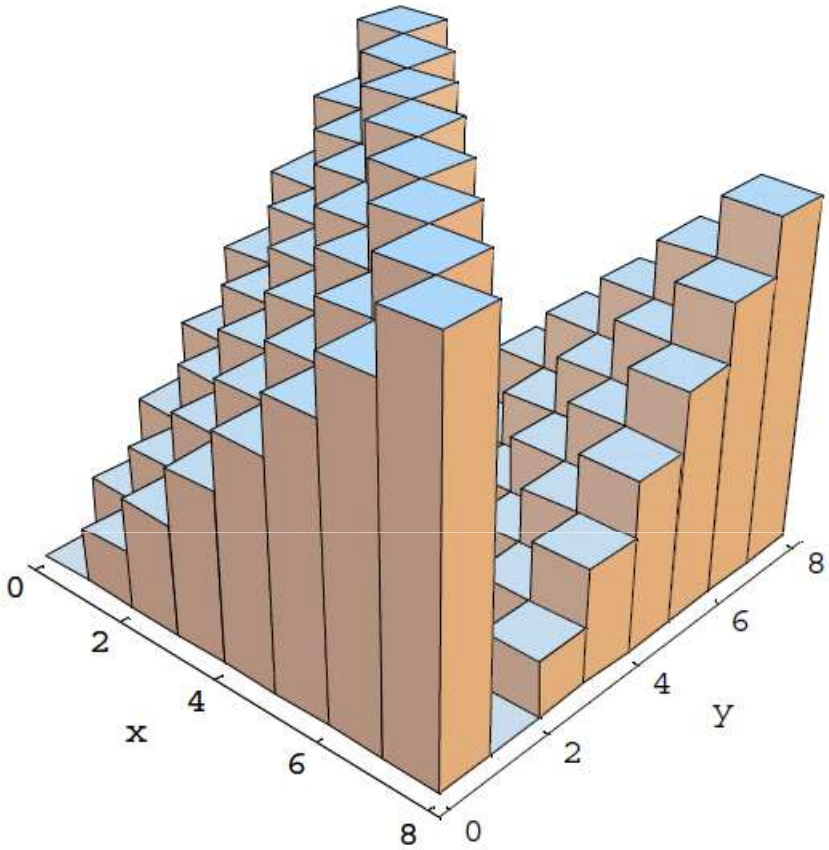


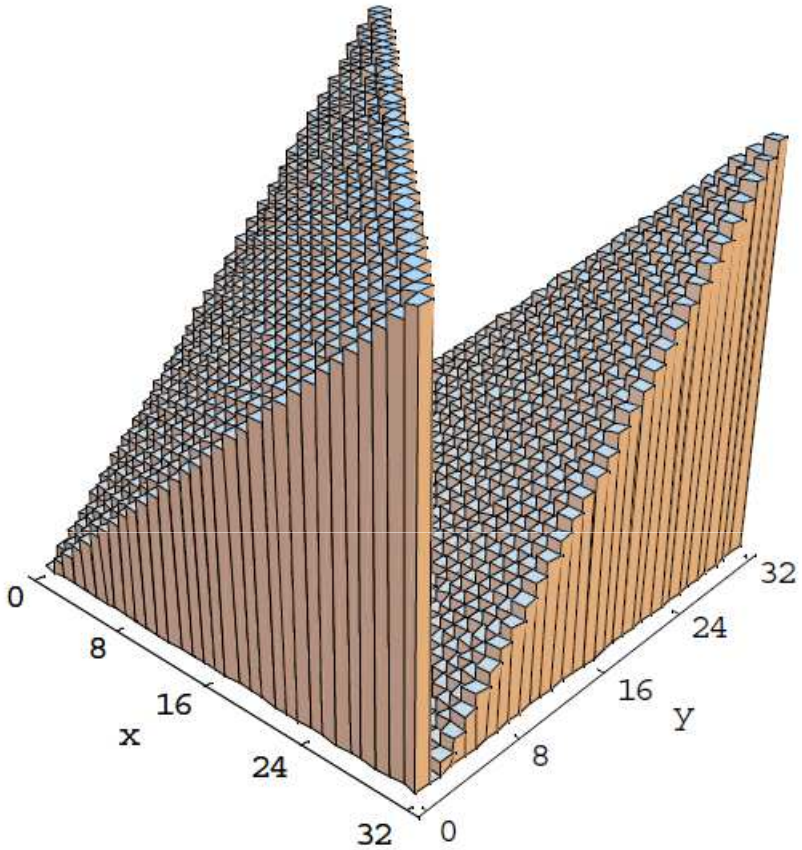
Регистр EFLAGS



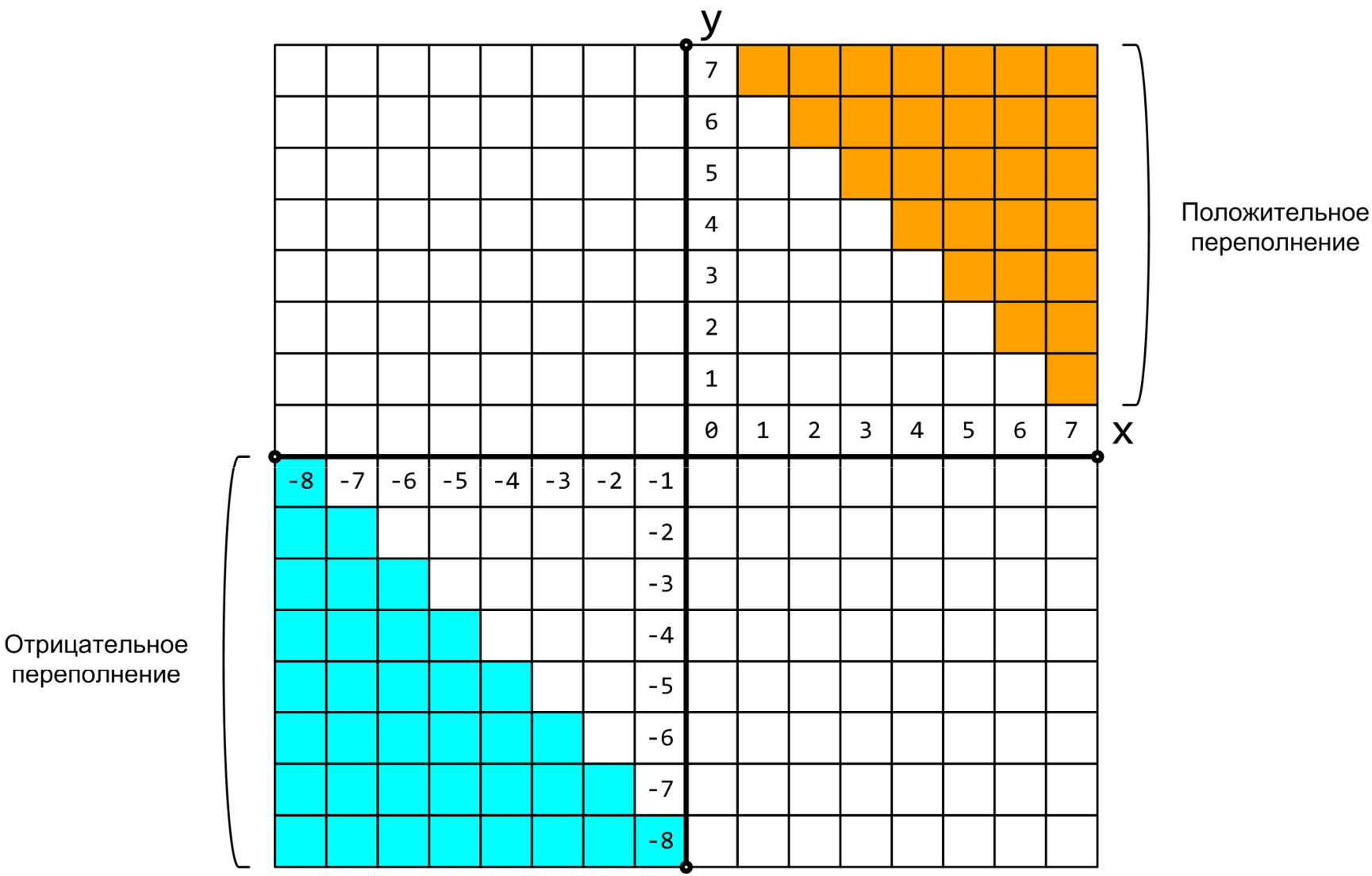
EFLAGS







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

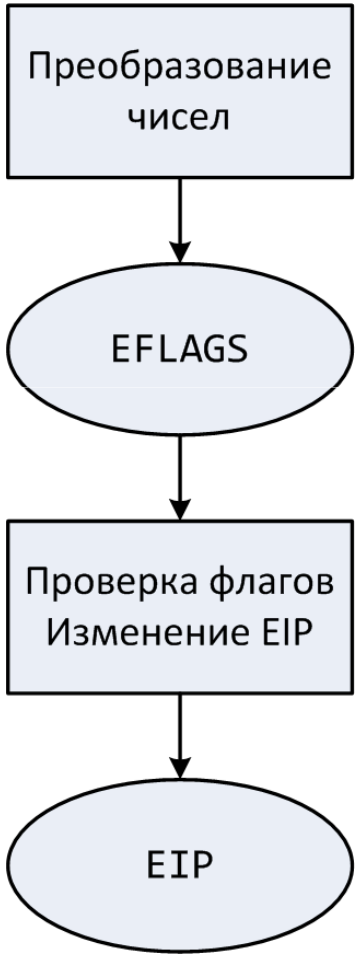


Естественный порядок выполнения

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

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



	OF	SF	ZF	PF	CF
ADD	M	M	M	M	M
SUB	M	M	M	M	M
IMUL MUL	M	-	-	-	M
IDIV DIV	-	-	-	-	-
NEG	M	M	M	M	M
CMP	M	M	M	M	M
TEST	-	M	M	M	-