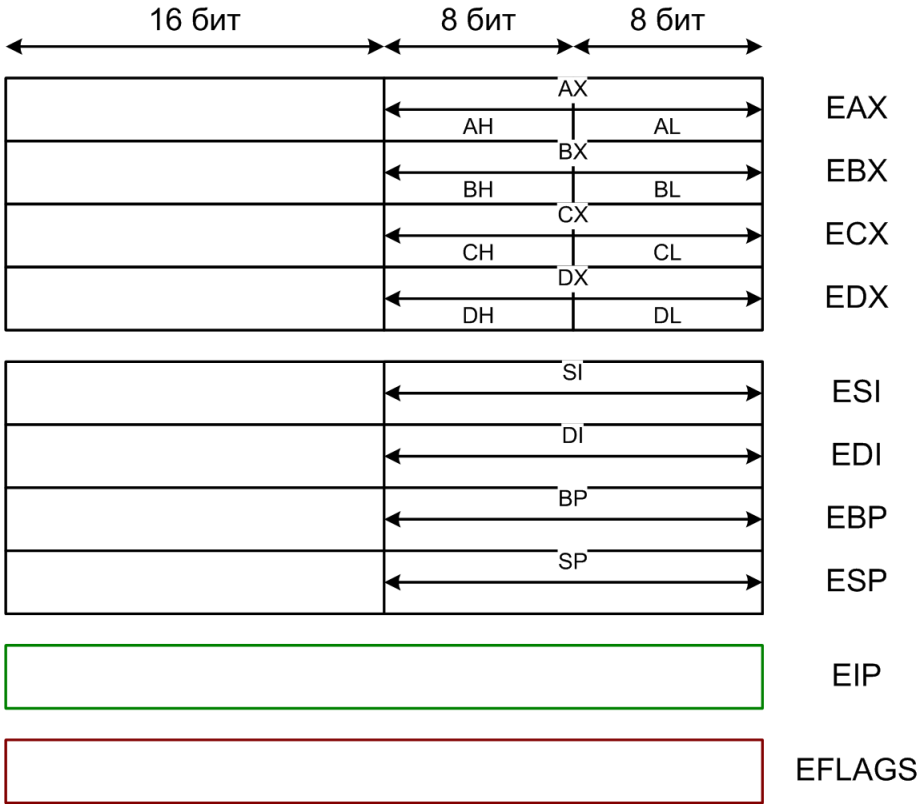
Лекция 4

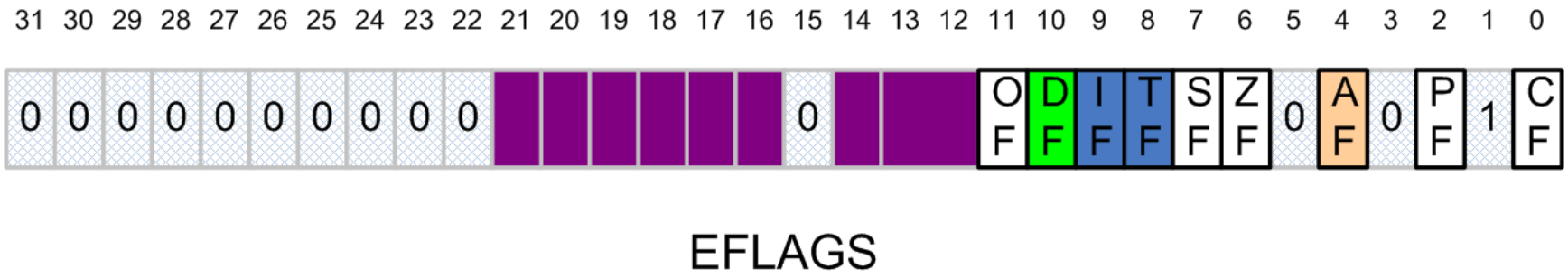
17 февраля

Основные арифметические команды

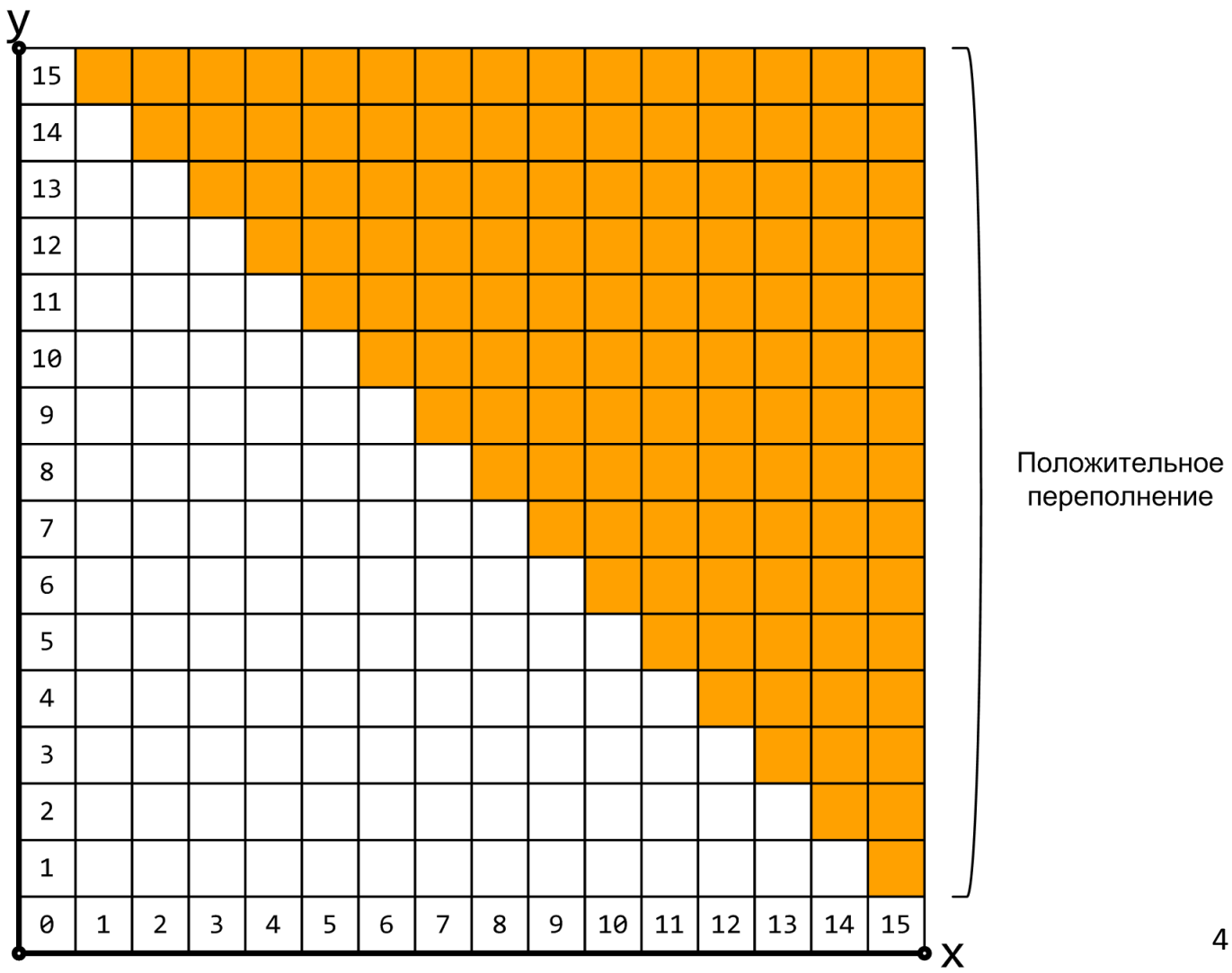
- MOV
- MOVSX, MOVZX
- ADD, SUB
- NEG
  - r/m 8/16/32
- MUL
  - r/m 8/16/32
- IMUL
  - r/m 8/16/32
  - r 16/32, r/m 16/32
  - r 16/32, r/m 16/32, i 16/32
- DIV, IDIV
  - r/m 8/16/32
- CBW, CWD, CDQ



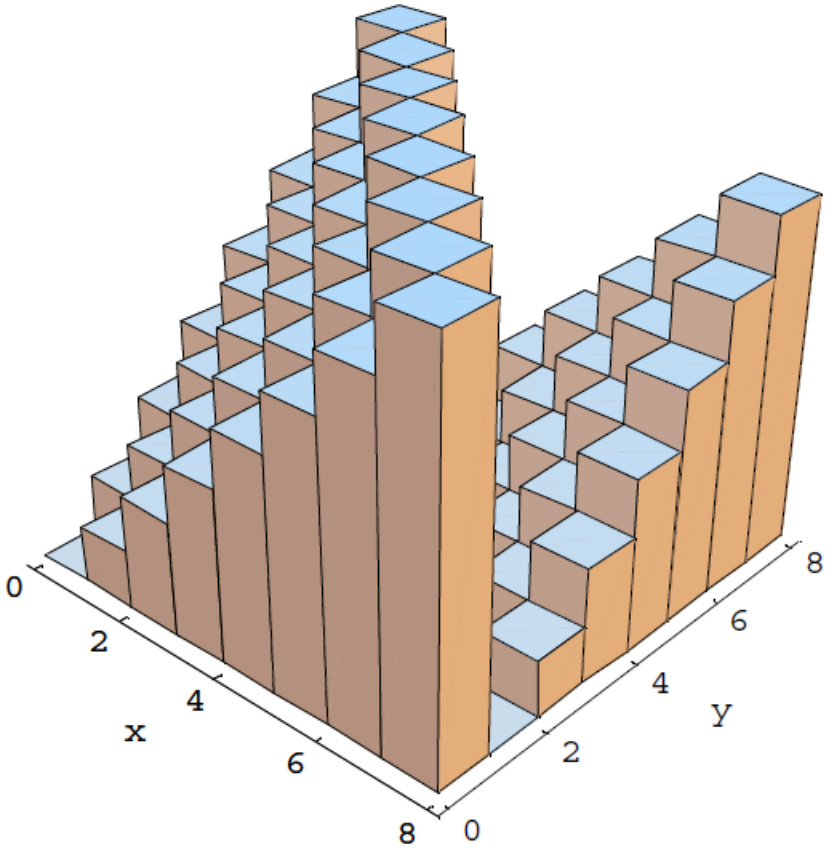
Регистр EFLAGS

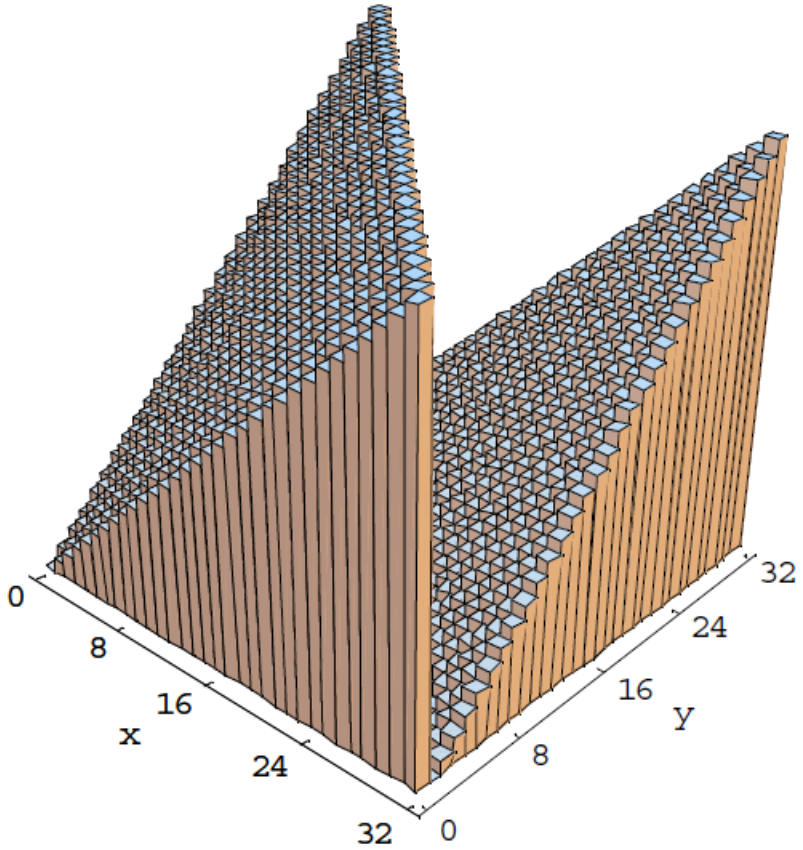


Переполнение при сложении двух беззнаковых чисел



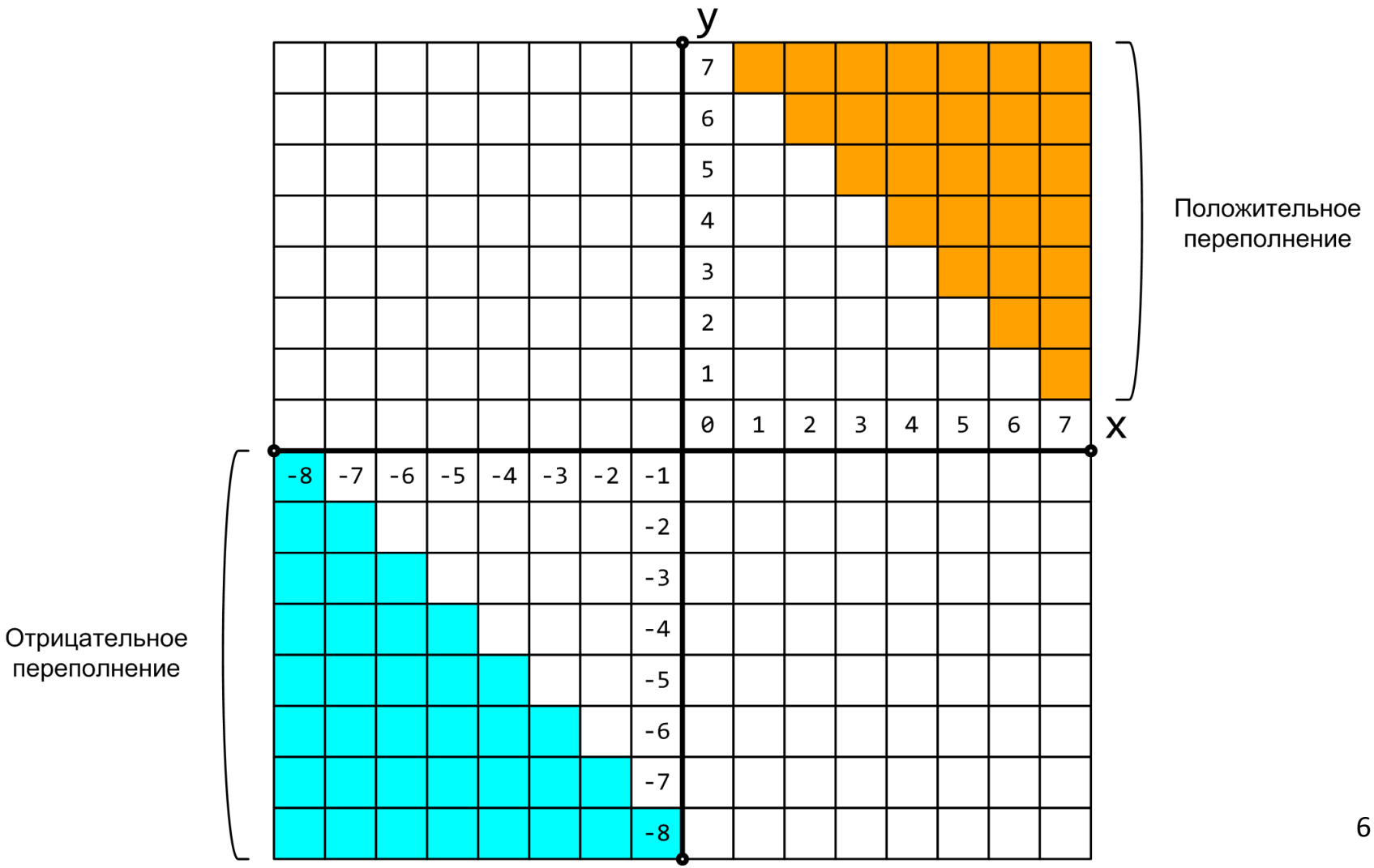
Как «выглядит» переполнение в 3D?





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

Переполнение при сложении двух знаковых чисел



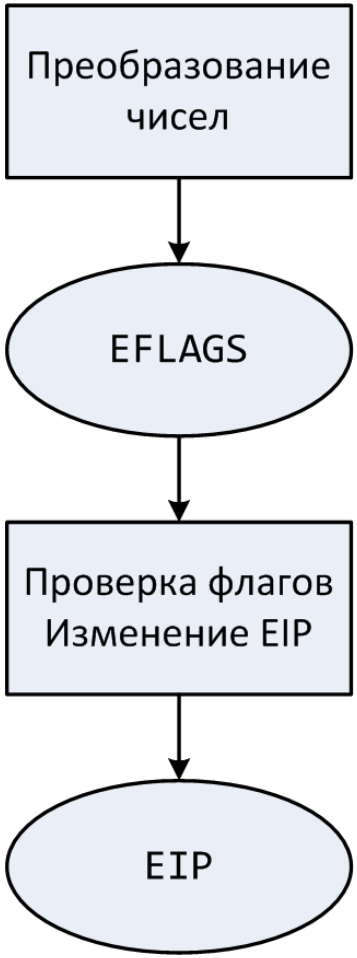
Естественный порядок выполнения

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

Изменение естественного порядка выполнения программы

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



Регистр EFLAGS и инструкции

	OF	SF	ZF	PF	CF
ADD, SUB, NEG	M	M	M	M	M
INC, DEC	M	M	M	M	
IMUL, MUL	M	–	–	–	M
IDIV, DIV	–	–	–	–	–
CBW, CWD, CDQ					
MOV, MOVSX, MOVZX					
CMP	M	M	M	M	M
TEST	0	M	M	M	0

«M» инструкция обновляет флаг (сбрасывает или устанавливает)
«–» влияние инструкции на флаг не определено
« » инструкция на флаг не влияет
«0» инструкция сбрасывает флаг