دوره مهندسی معکوس نرم افزار

- Site: OnHexGroup.ir
- Youtube: @onhexgroup
- Telegram: onhex_ir
- Twitter: @onhexgroup
- Github: onhexgroup

نسخه ی ۳۲ و ۶۴ بیتی

پلتفرم: ویندوز

ارائه دهنده : **OnhexGroup**

Onhexgroup.ir

دستور ADD

- دستور **ADD** برای جمع دو عملوند استفاده میشه.
- عملکرد این دستور:

ADD OP1,OP2

OP1=OP1+OP2

- روی فلگ های **PF,AF,ZF,SF,OF,CF** تاثیر میزاره.

ADD R/M,R/M/IMM

Onhexgroup.ir

دستور SUB

- دستور **SUB** برای تفریق دو عملوند استفاده میشه.
- عملکرد این دستور:

SUB OP1,OP2

OP1=OP1-OP2

- روی فلگ های **PF,AF,ZF,SF,OF,CF** تاثیر میزاره.

SUB R/M,R/M/IMM

Onhexgroup.ir

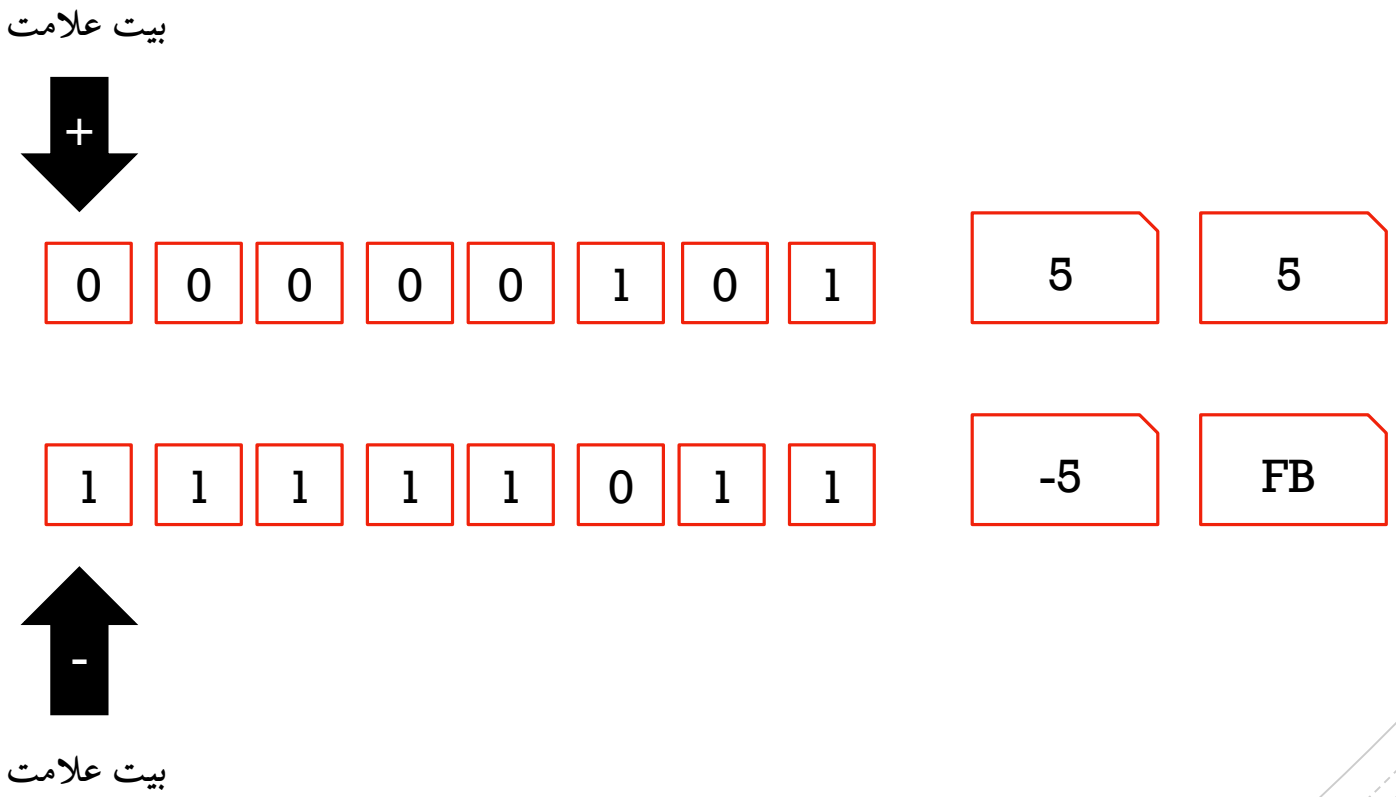
اعداد با علامت و بدون علامت

- منظور از اعداد بدون علامت اعداد مثبت و منظور از اعداد با علامت اعداد مثبت و منفی هستش.
- نکات مهم اعداد:
  - نمایش اعداد علامتدار
  - تبدیل مثبت به منفی و منفی به مثبت
  - محدوده اعداد
  - تشخیص مثبت و منفی بودن

- در دسیمال ۱۱ و ۱۱-
- در سیستم های دیجیتال:

Onhexgroup.ir

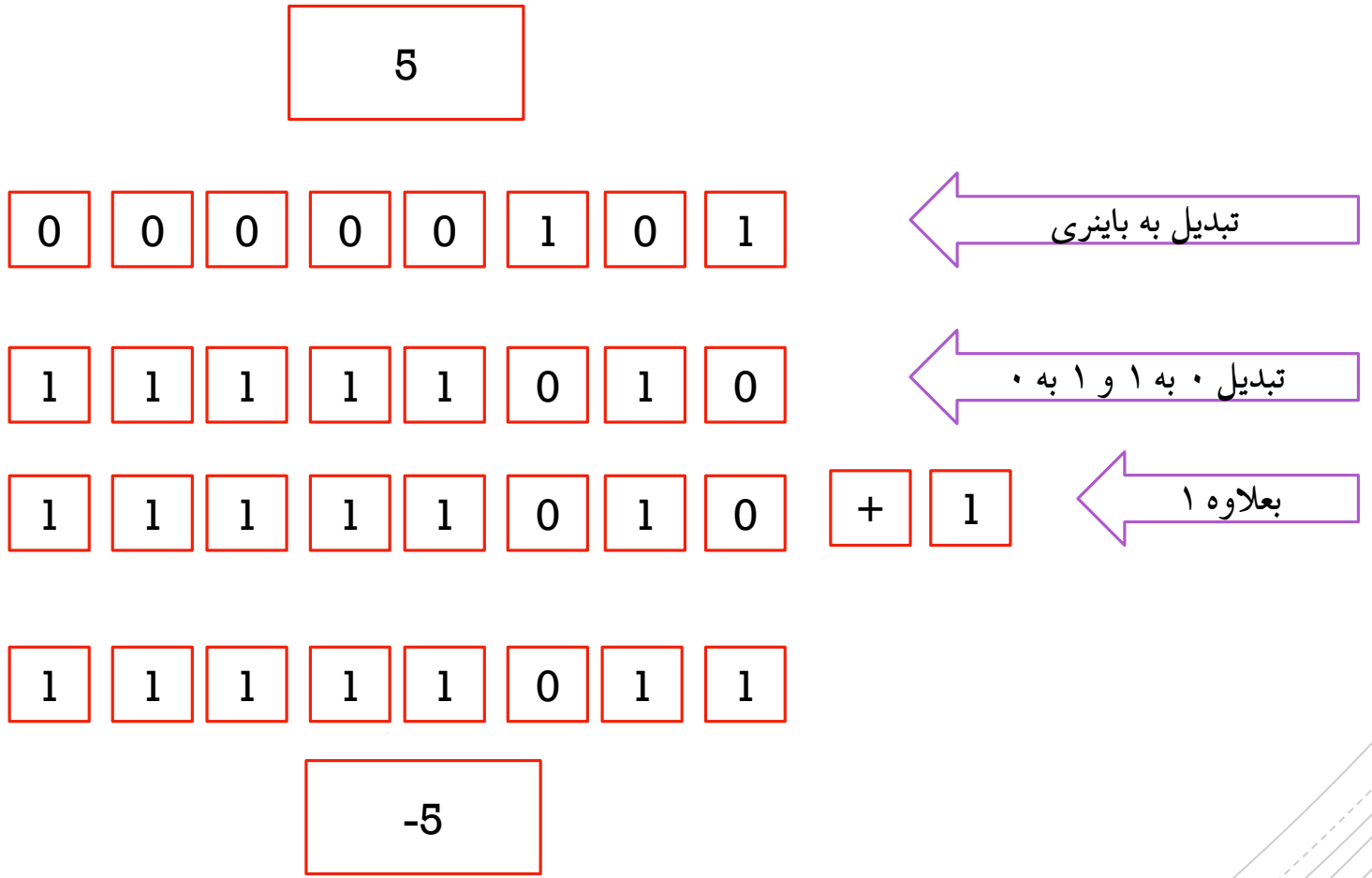
نمایش اعداد علامتدار



- در دسیمال ۱۱ و ۱۱-
- در سیستم های دیجیتال: (مکمل ۲)

Onhexgroup.ir

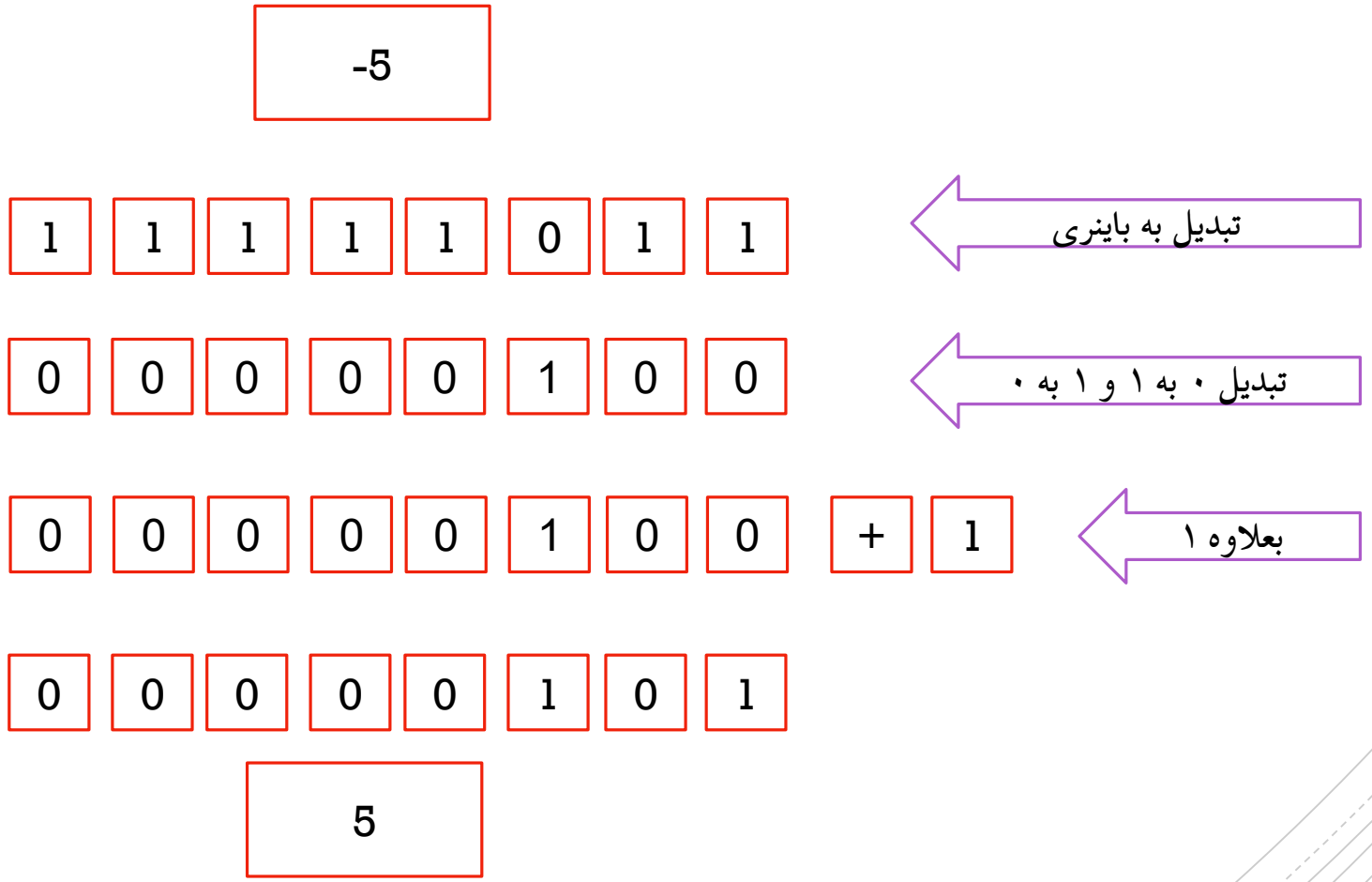
تبدیل مثبت به منفی



- **در سیستم های دیجیتال: (مکمل ۲)**

Onhexgroup.ir

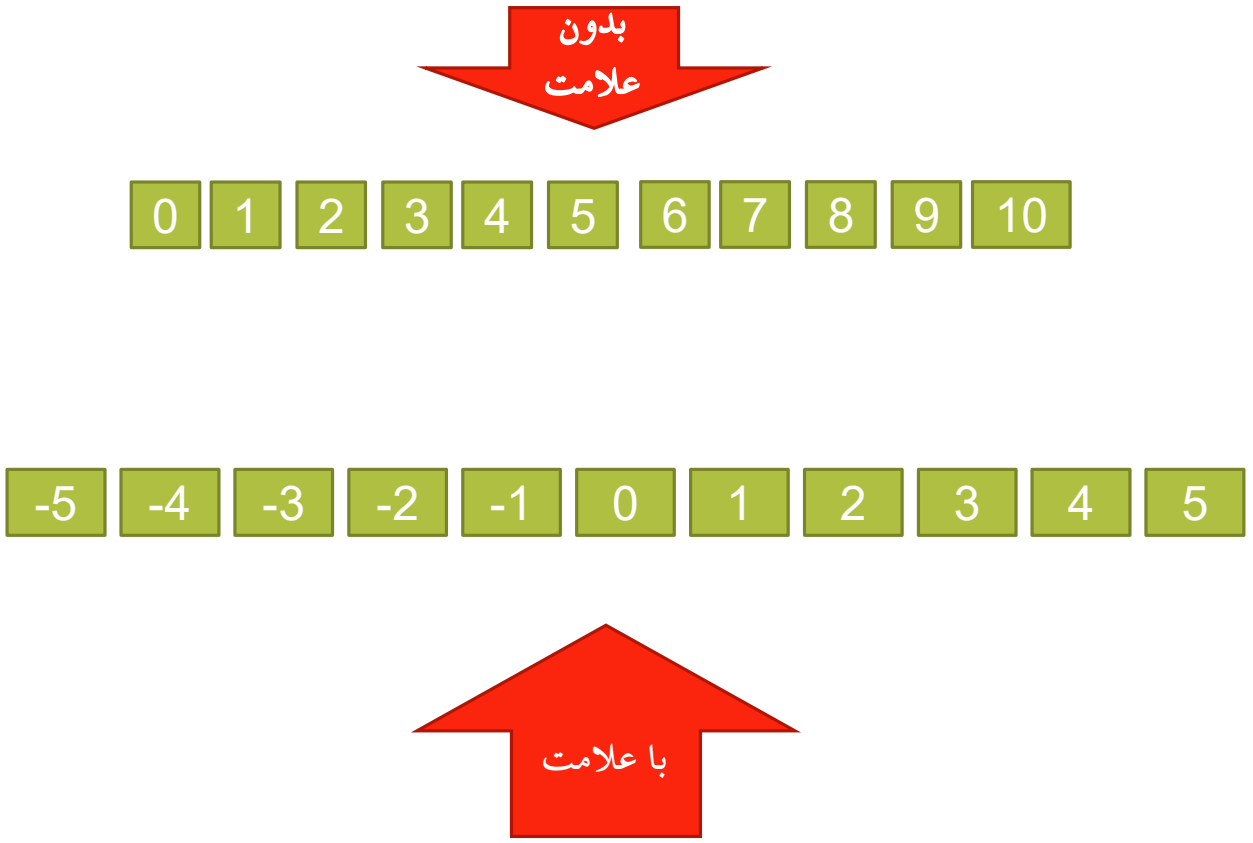
تبدیل منفی به مثبت



Onhexgroup.ir

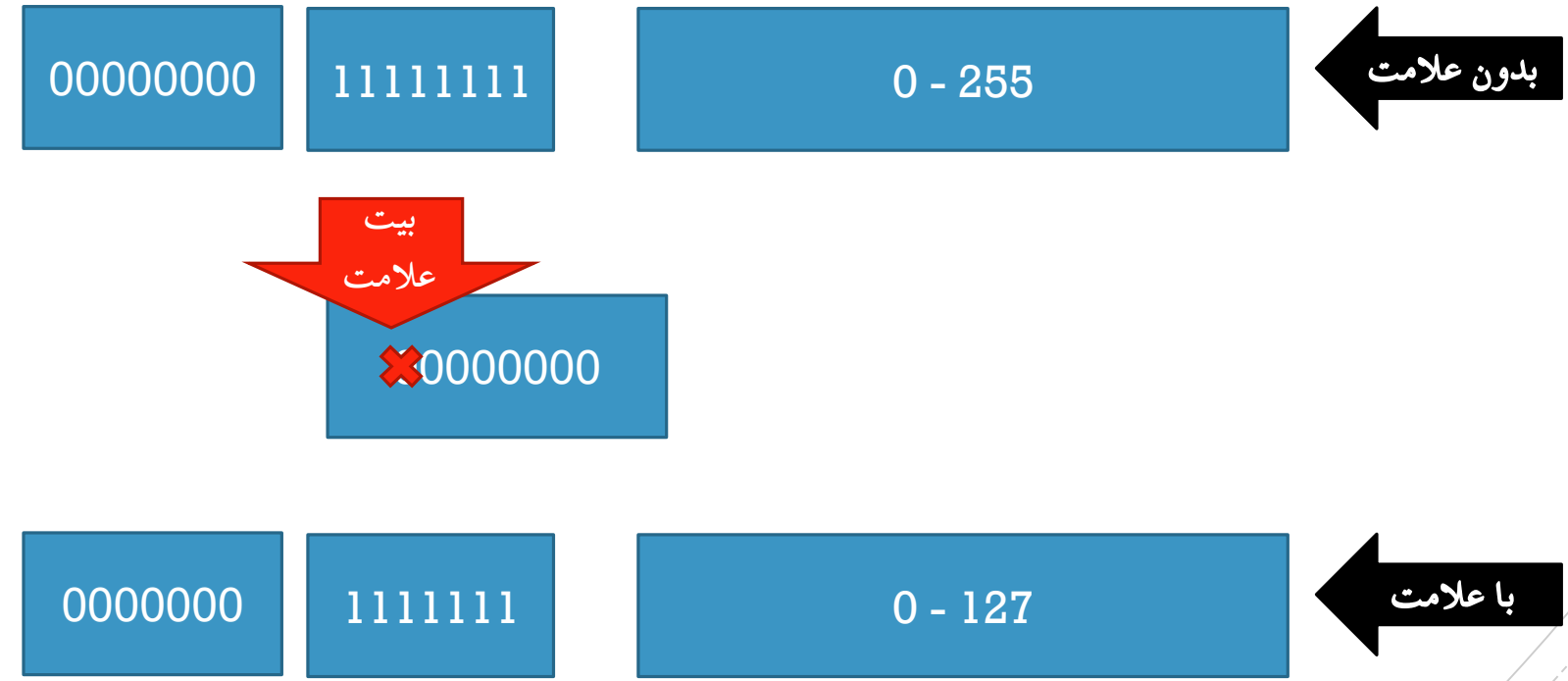
محدوده اعداد

- فرض کنید یک بازه عددی ۱۱ تایی از شما خواستن:



Onhexgroup.ir

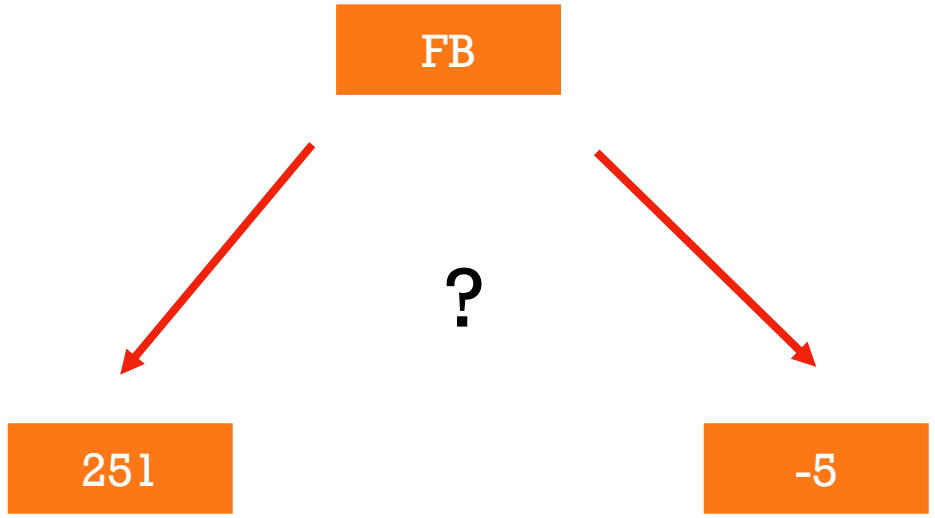
محدوده اعداد



Onhexgroup.ir

تشخیص مثبت و منفی

Mov AL,0FBh



Onhexgroup.ir

تشخیص مثبت و منفی

- ۱-نوع دستورات بعدی و قبلی
  - دستورات **imul** و **idiv** و **jl** و **jg** و **movsx** برای علامت دار
  - دستورات **mul** و **div** و **jb** و **ja** و **movzx** برای بدون علامت
- ۲- نوع داده
- ۳- بیت علامت (فلگ)
- ۴- عملکرد خود برنامه

Onhexgroup.ir

جمع باینری

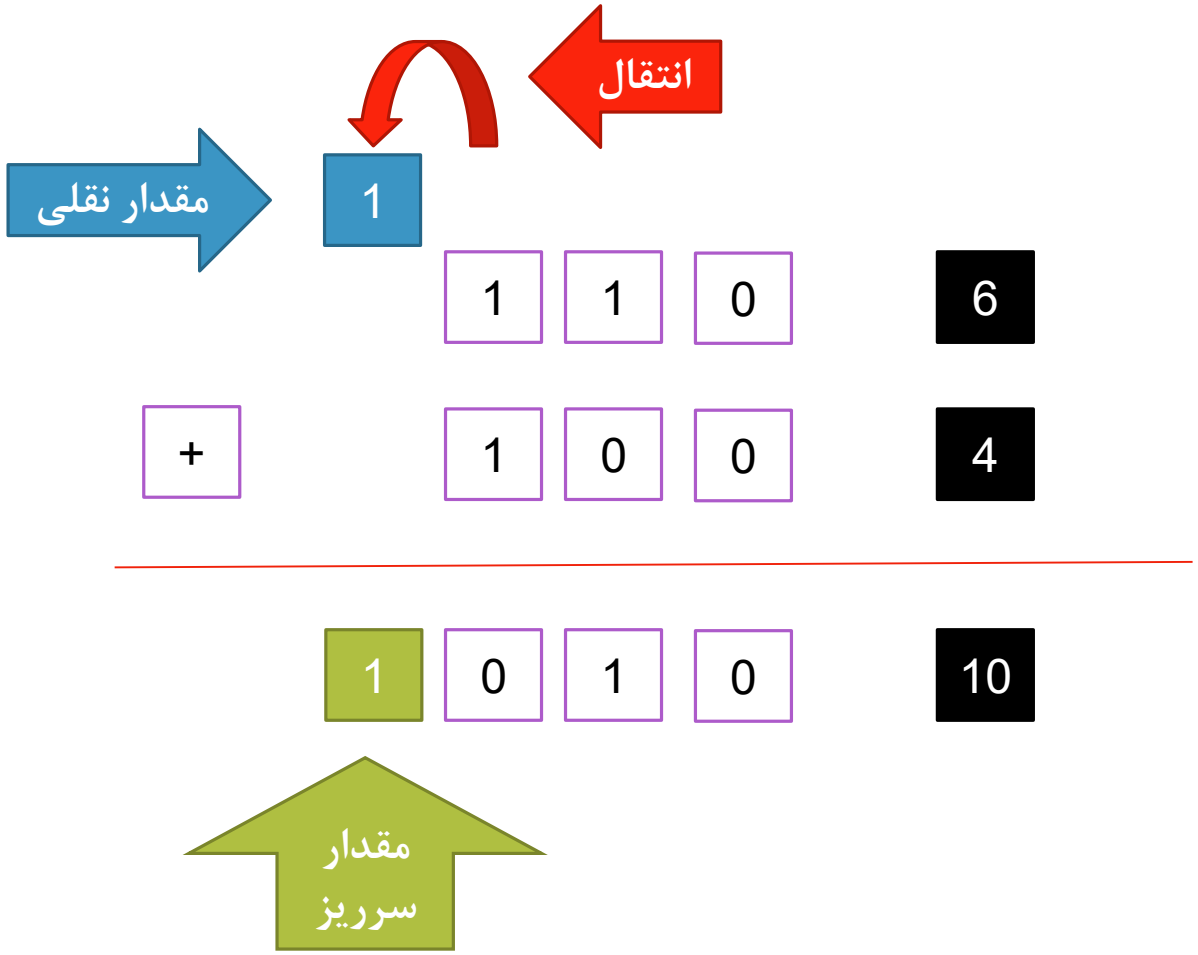
- حالتهای مختلف عمل جمع:

عدد اول	عدد دوم	نتیجه	نقلی	مثال
0	0	0	0	0+0=0
0	1	1	0	0+1=1
1	1	0	1	1+1=0
1+1	1	1	1	1+1+1=1

1+1=2=10
1+1+1=3=11

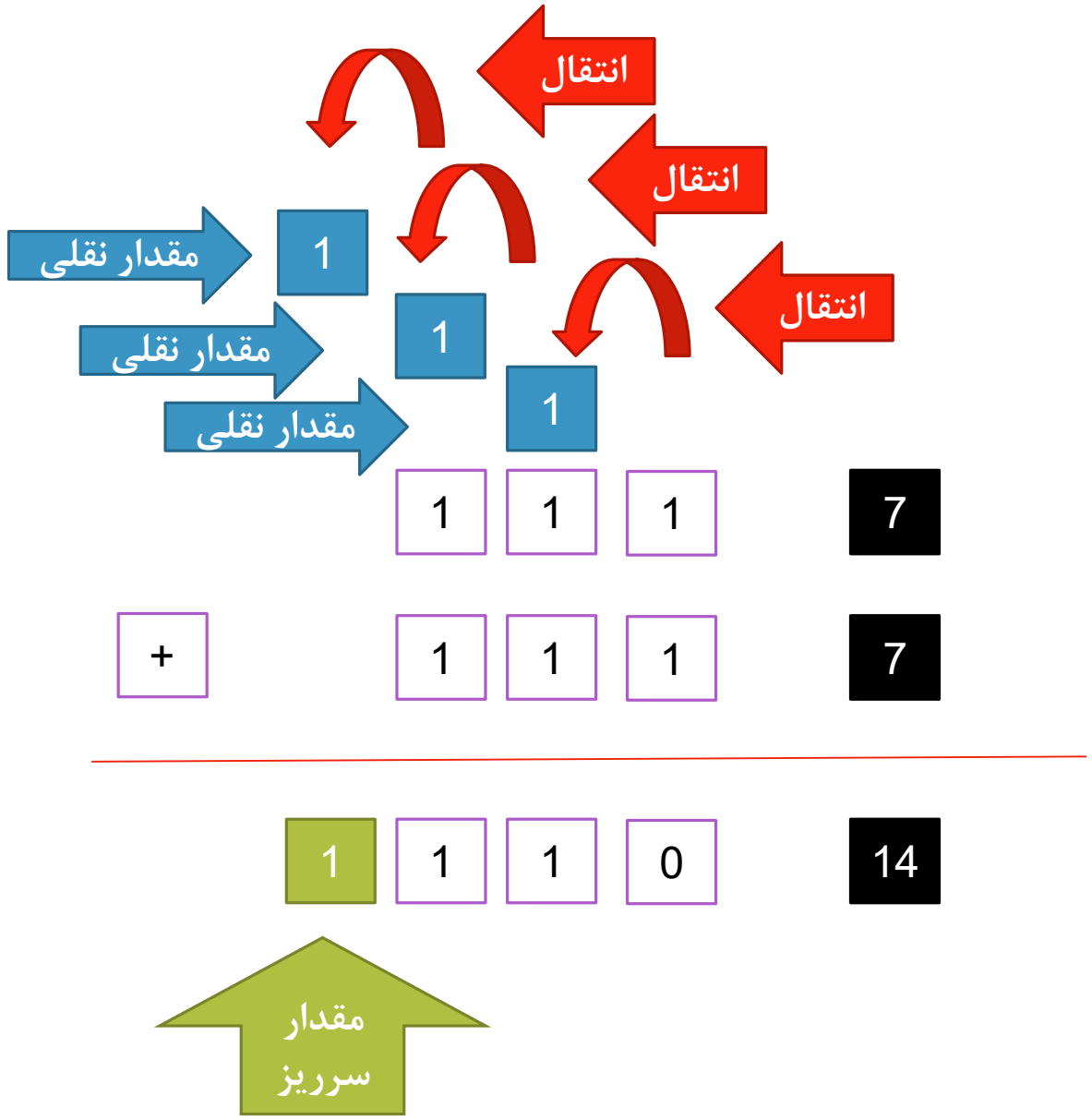
Onhexgroup.ir

جمع باینری



Onhexgroup.ir

جمع باینری



Youtube: Onhexgroup

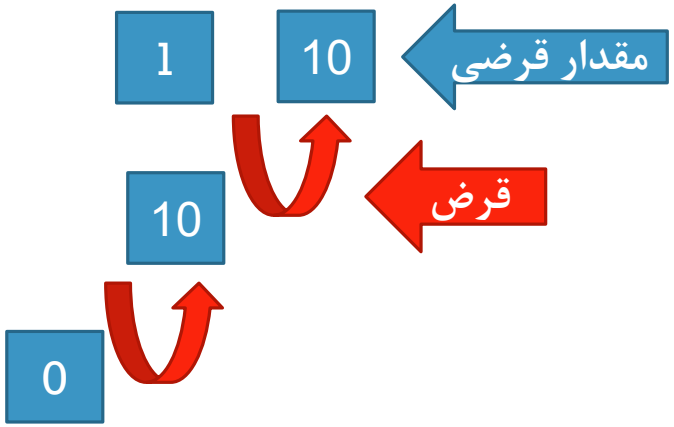
تفریق باینری

- حالتهای مختلف عمل تفریق:

عدد اول	عدد دوم	نتیجه	قرض	مثال
0	0	0	0	0-0=0
1	1	0	0	1-1=0
1	0	1	0	1-0=1
0	1	1	2	0-1=1

10-1=1

- تفریق اعداد بدون علامت



	1	0	0	1	9
-	0	1	1	1	7
	0	0	1	0	2

Github:Onhexgroup

تفریق باینری

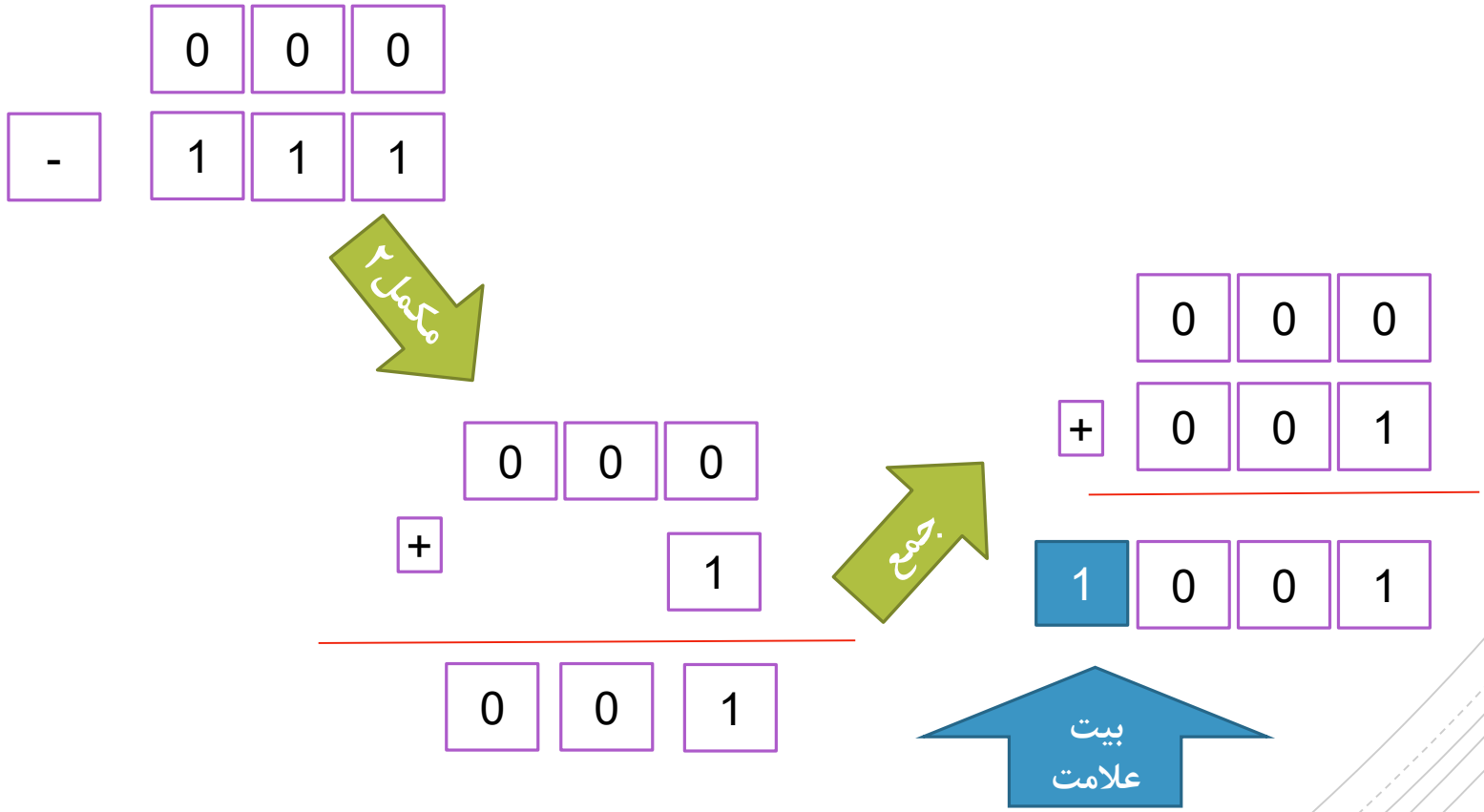
- تفریق اعداد باعلامت

000-111=?

0-7= 0 + (-7) = -7

Twitter: Onhexgroup

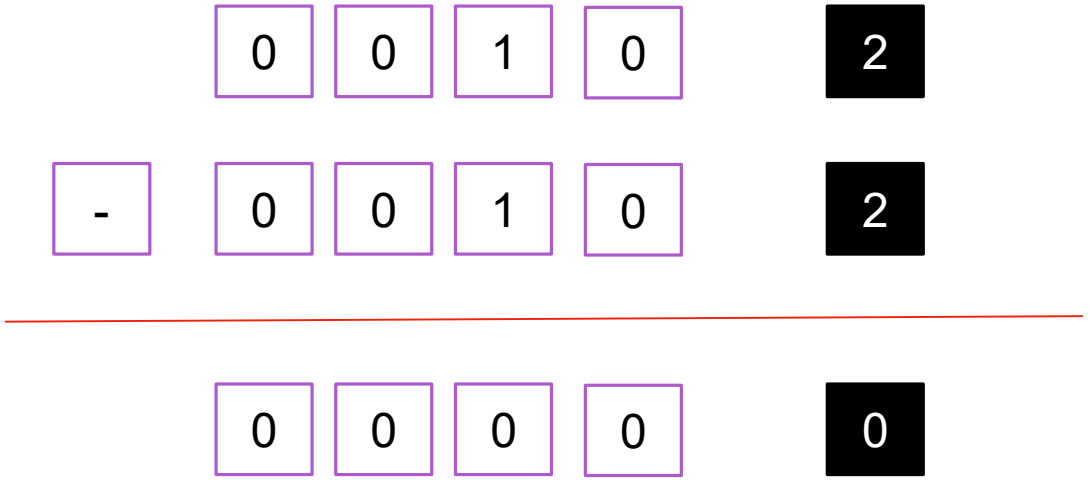
تفریق باینری



Onhexgroup.ir

فلگها

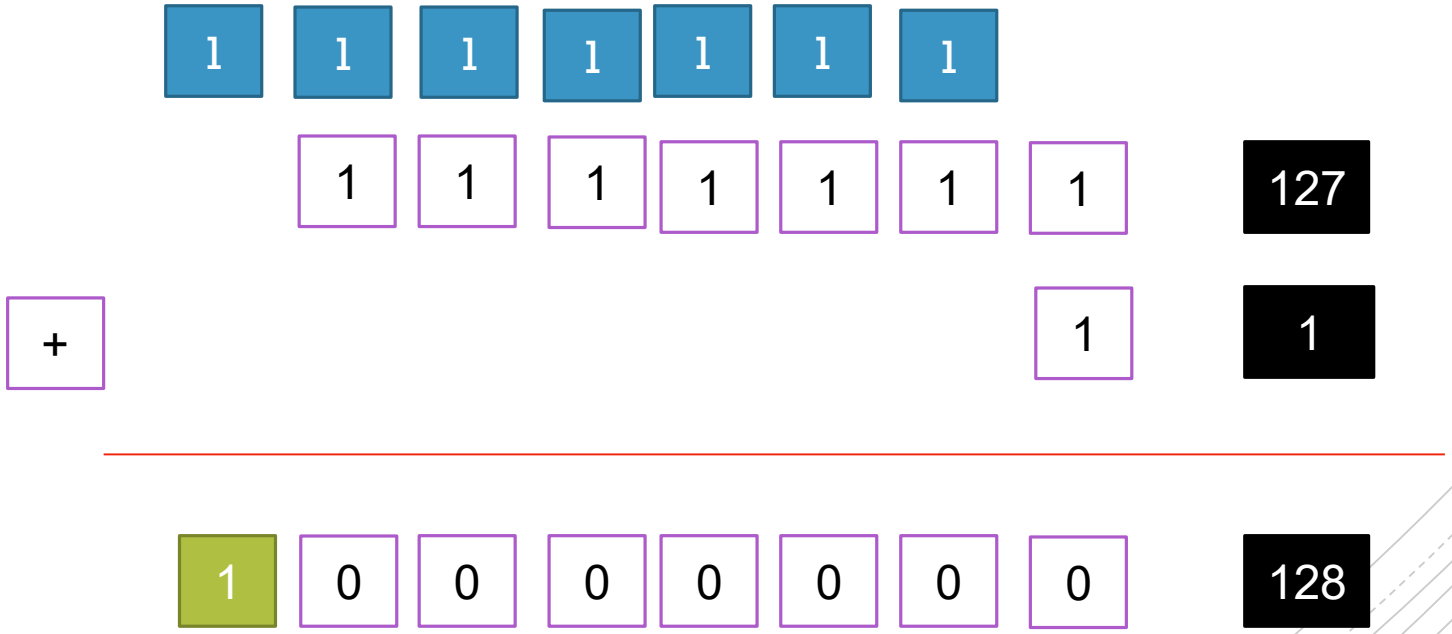
- **Zero Flag (ZF)** : نشون دهنده صفر بودن نتیجه ی عملیات
  - مقدار ۰: اگه نتیجه عملیات غیر صفر باشه.
  - مقدار ۱: اگه نتیجه عملیات صفر باشه.
  - در ویژوال استدیو با **ZR** مشخص میشه. (؟**NZ**)



Youtube: Onhexgroup

فلگها

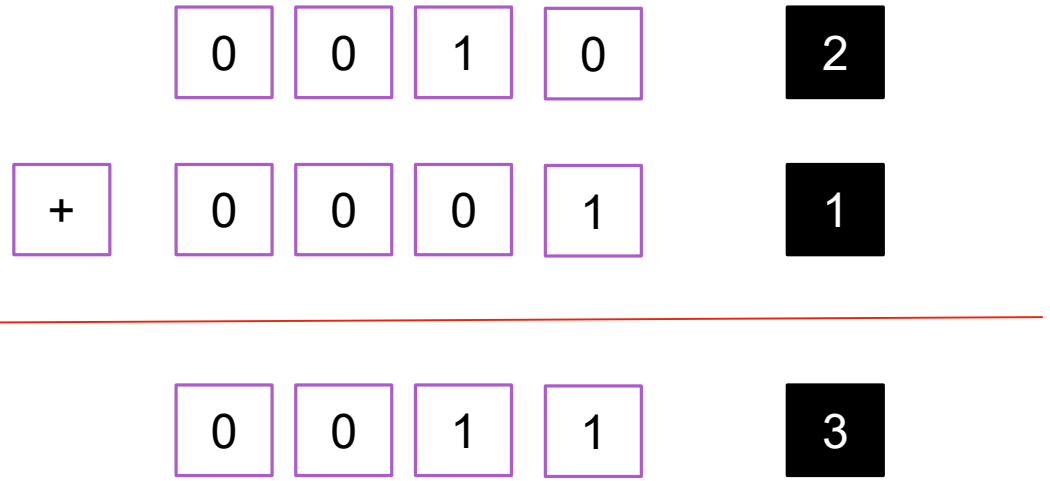
- **Overflow Flag (OF)**: نشون دهنده سرریزه در عملیات علامتدار – یعنی نتیجه خارج از محدوده باشه.
  - مقدار ۰: خارج از محدوده نیست
  - مقدار ۱: خارج از محدوده است.
  - در ویژوال استدیو با **OV** مشخص میشه.



Twitter: Onhexgroup

فلگها

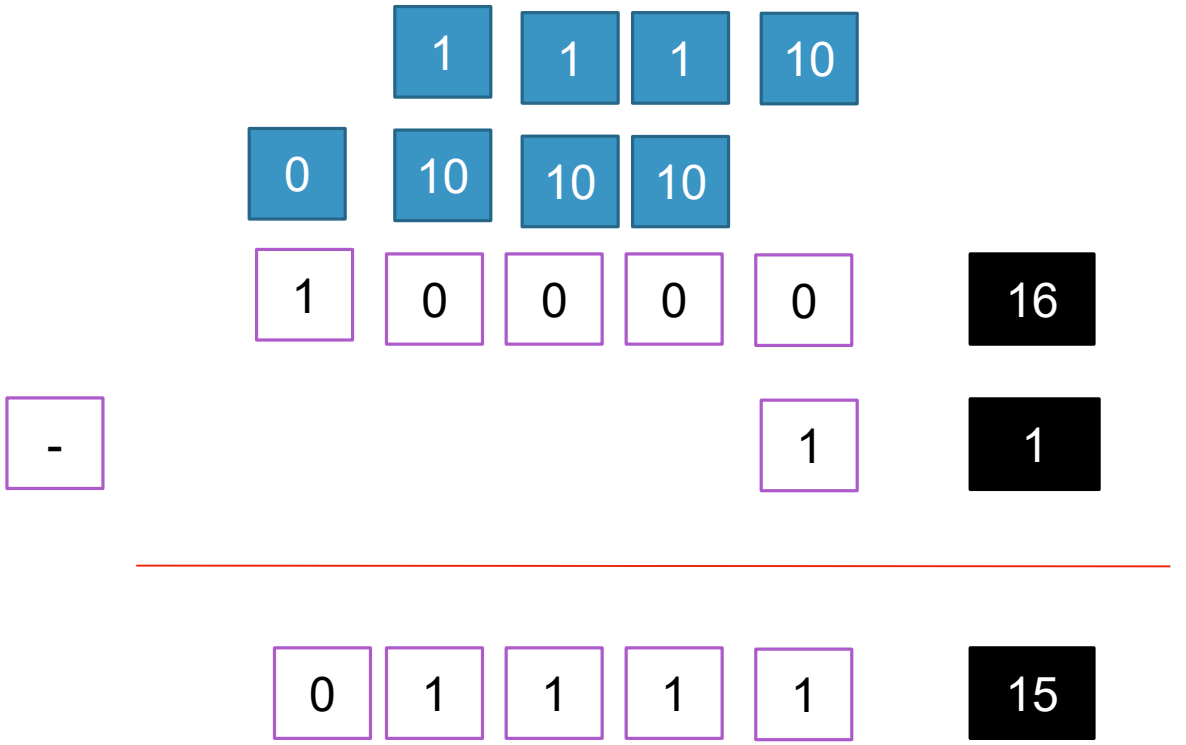
- **Parity Flag (PF)** : نشون دهنده زوج یا فرد بودن بیت های یک در نتیجه عملیات
  - مقدار ۰: تعداد یک ها فرد است
  - مقدار ۱: تعداد یک ها زوج است.
  - در ویژوال استدیو با **PE** مشخص میشه.



Github: Onhexgroup

فلگها

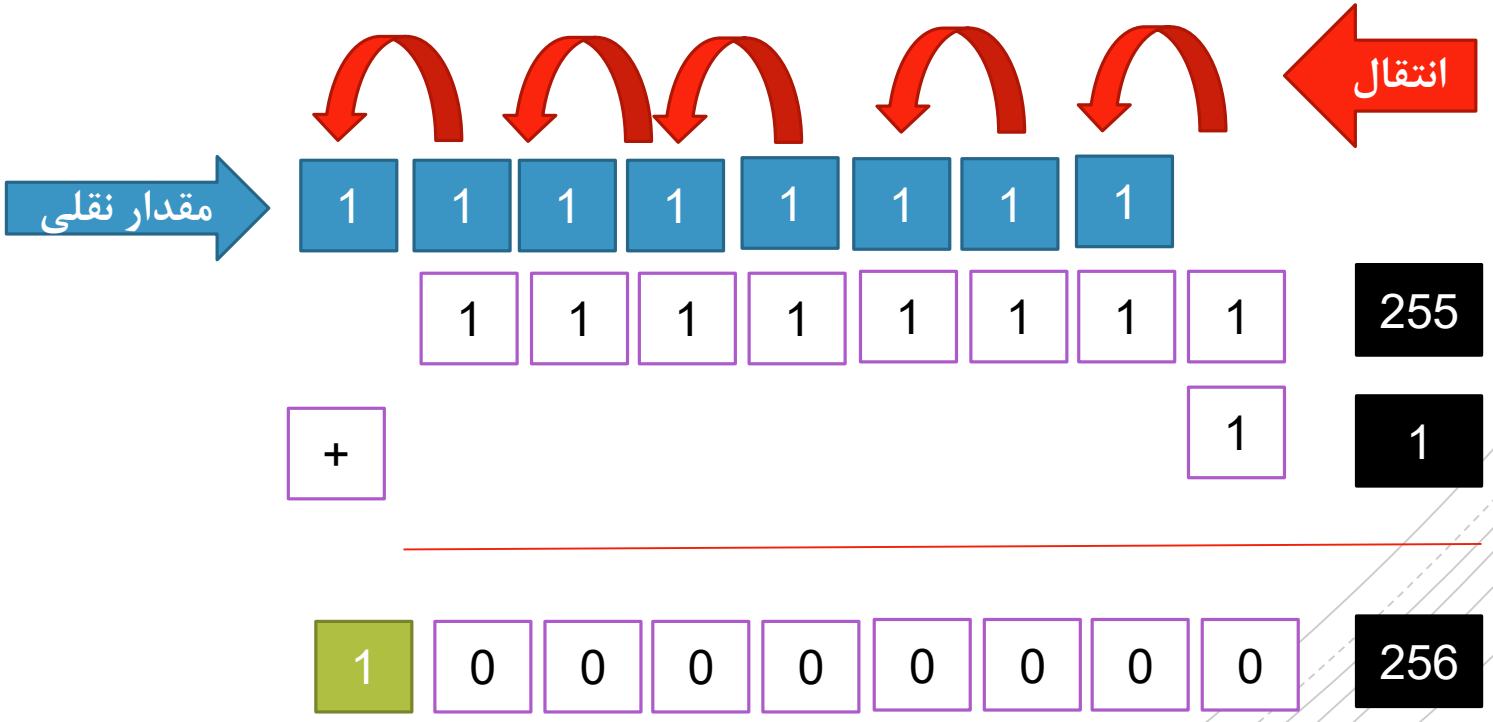
- **AF - Auxiliary Flag**:
  - در جمع : نشون دهنده انتقال در بیت ۳ به بیت ۴
  - در تفریق: نشون دهنده قرض در بیت ۴ به بیت ۳
  - در ویژال استدیو با **AC** مشخص میشه.



Insta: Onhexgroup

فلگها

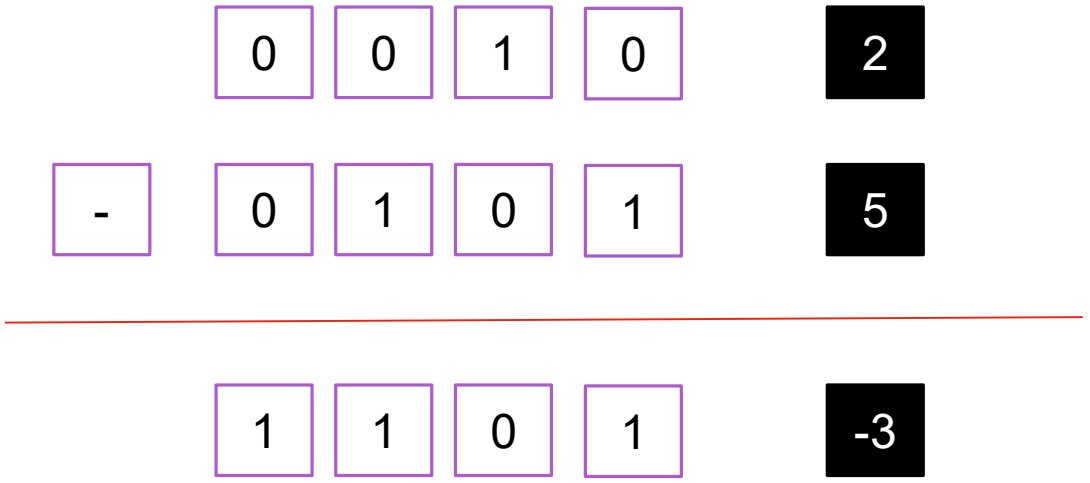
- **Carry Flag (CF)** :
  - در جمع بدون علامت : اگه ۱ باشه یعنی مقدار نقلی از بیت با ارزش داریم.
  - در تفریق بدون علامت: اگه مقدار رقم دوم بزرگتر از رقم اول باشه برابر ۱ میشه.
  - در ویژوال استدیو با **CY** مشخص میشه.



Youtube: Onhexgroup

فلگها

- **Sign Flag (SF)**: نشون دهنده علامت نتیجه عملیات
  - مقدار ۰: مشخص کننده مثبت
  - مقدار ۱: مشخص کننده منفی
  - در ویژوال استدیو با **PL** مشخص میشه.



Onhexgroup.ir

دستور XADD

- دستور **XADD** برای جمع و جا به جایی دو عملوند استفاده میشه.
- عملکرد این دستور:

XADD OP1,OP2

OP2=OP1

OP1=OP1+OP2

- روی فلگ های **CF, PF, AF, SF, ZF,OF** تاثیر میزاره.

XADD R/M,R

Youtube: Onhexgroup

دستور INC

- دستور **INC** یک واحد به مقدار گرفته شده اضافه میکنه. **(i++)**
- عملکرد این دستور:

INC OP

OP=OP+1

- روی فلگ های **OF, SF, ZF, AF, PF** تاثیر میزاره.

INC R/M

Twitter: Onhexgroup

دستور DEC

- دستور **DEC** یک واحد از مقدار گرفته شده کم میکنه. (**i--**)
- عملکرد این دستور:

DEC OP

OP=OP-1

- روی فلگ های **OF, SF, ZF, AF, PF** تاثیر میزاره.

DEC R/M

Telagram: onhex_ir

درصد

ONHEXGROUP

54%

NOP 10%	PUSH 15%	CALL 8%	LEA 5%
MOV 27%	INT3 5%	ADD 3%	JNZ 2%
POP 3%	JMP 2%	XOR 2%	XADD 1%
CMP 3%	JG 1%	DEC 1%	JZ 2%
TEST 3%	RET 2%	SUB 2%	OTHRES 5%