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

زبان اسمبلی

- زبان سطح پایین
- توسط اسمبلر به زبان ماشین قابل اجرا تبدیل میشه
- بدلیل سخت بودن زبان ماشین توسعه داده شد.
  - کد زبان ماشین زیر :

10110000 01100001

  - معادل هگز :

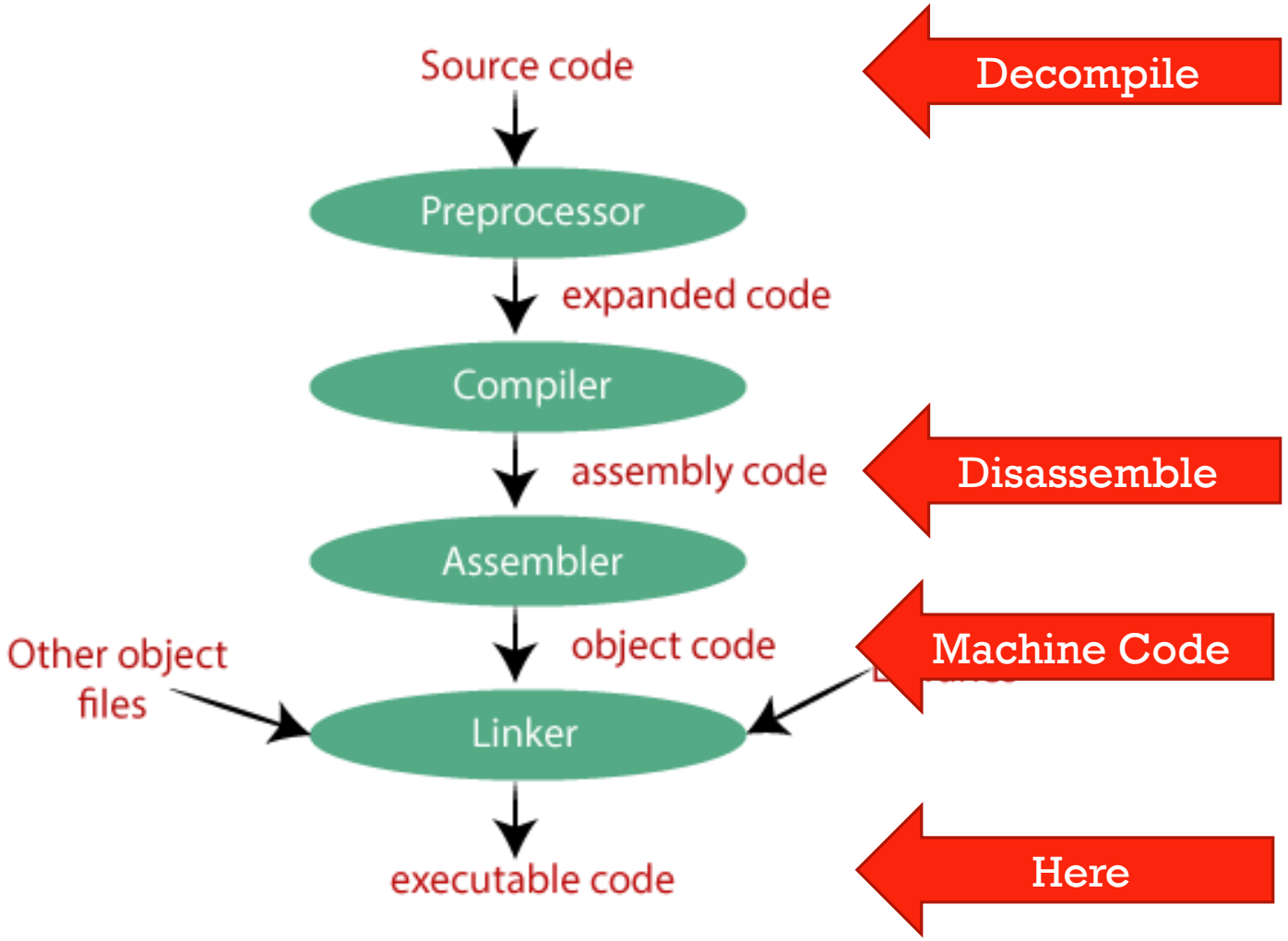
B0 61

  - اسمبلی :

MOV AL, 61h

Onhexgroup.ir

اهمیت یادگیری زبان اسمبلی



Onhexgroup.ir

نحوه ی یادگیری اسمبلی

- مانند یادگیری زبان خارجه برای بزرگترهاست
- مهم درک کد هست نه نوشتن !

Onhexgroup.ir

قالب دستورات اسمبلی

- شکل کلی دستورات زبان اسمبلی بصورت زیر هستش :

```
Label Instruction  opr1,Opr2,... ;comment

Add 1,2   ; jameh 1+2
jump chap
Add 2,1 ...
...

Chap:
        Print Time          ; Time ra chap mikone
        Print "Tamam"   ; chizi ra chap mikone
```

Onhexgroup.ir

سینتکس دستورات اسمبلی

- دو سینتکس رایج داریم:
  - Intel
  - AT&T

AT&T		Intel		توضیحات
movl	$1,%eax	mov	eax,1	پیشوند
movl	(%ecx),%eax	mov	eax,[ecx]	مبدا و مقصد
movl	(%ebx),%eax	mov	eax,[ebx]	عملگر ممووری
movl	3(%ebx),%eax	mov	eax,[ebx+3]	
movb	%bl,%al	mov	al,bl	پسوند
movw	%bx,%ax	mov	ax,bx	
movl	%ebx,%eax	mov	eax,ebx	
movl	(%ebx),%eax	mov	eax, dword ptr [ebx]	

Onhexgroup.ir

اساس دوره

- در این دور ما موارد زیر رو پوشش میدیم:
  - پردازنده های خانواده X86
  - نسخه ی ۳۲ بیتی و ۶۴ بیتی رو پوشش میدیم.
  - در حالت Protected Mode هستیم
  - مهندسی معکوس برنامه های کامپایلری (C/C++)
  - نمایش در حافظه بصورت Little Endian خواهد بود.
  - سینتکس مورد نظر Intel

Onhexgroup.ir

دستورات مهم اسمبلی

- درک دستورات مهم هستش.
- عنوان تحقیق :
  - An Analysis of x86-64 Instruction Set for Optimization of System Softwares
  - سال ۲۰۱۱
  - برنامه :
    - **Acrobat.exe**
    - **Explorer.exe**
    - **IExplorer.exe**
    - **Maya.exe**
    - **Mpc-hc.exe**
    - **Opera.exe**
    - **PES2010.exe**
    - **WinRAR.exe**
    - **Wordpad.exe**
    - و ...

Onhexgroup.ir

دستورات مهم اسمبلی

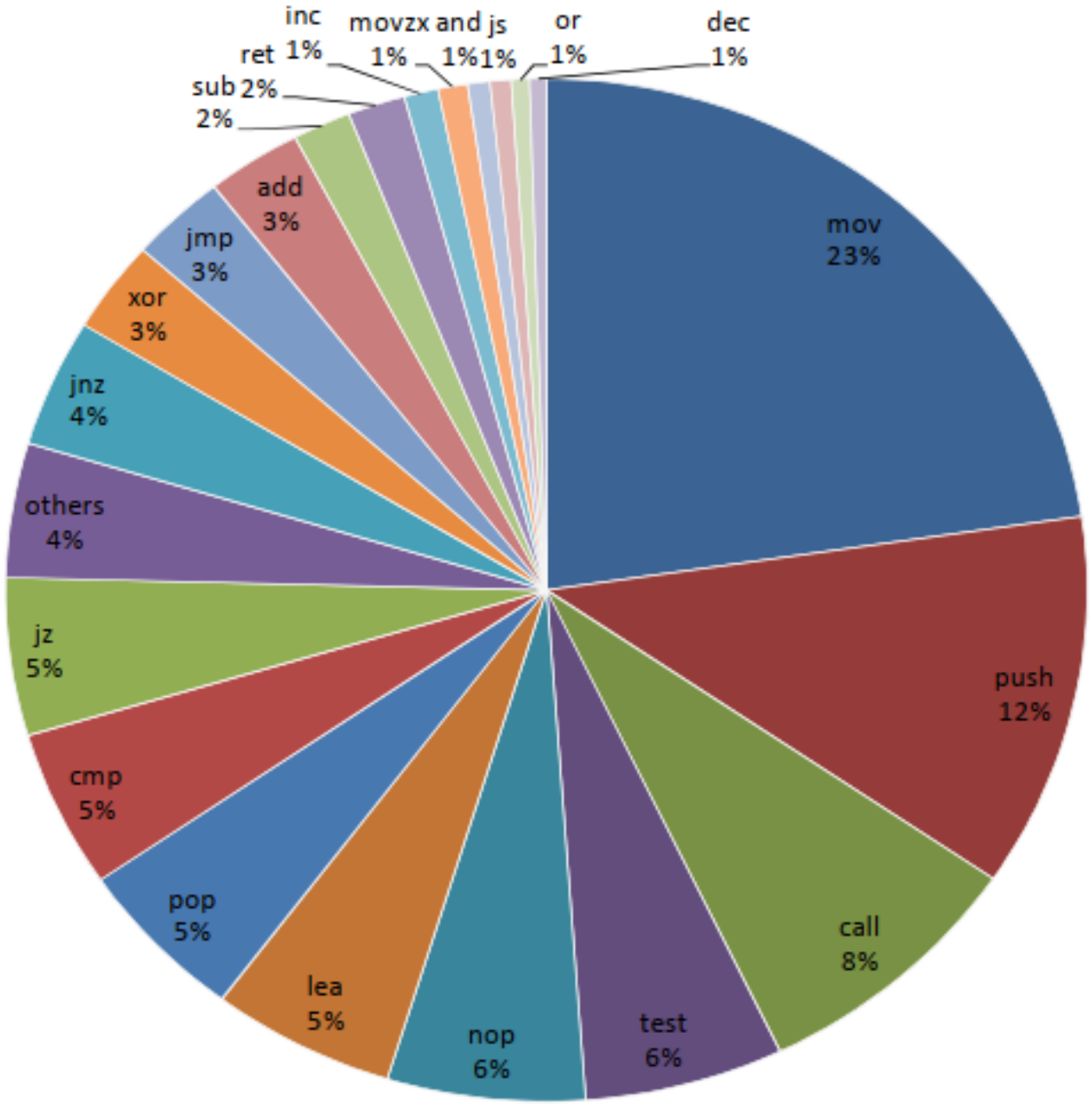


Fig. 2 Web browsers' instruction frequencies

Onhexgroup.ir

دستورات مهم اسمبلی

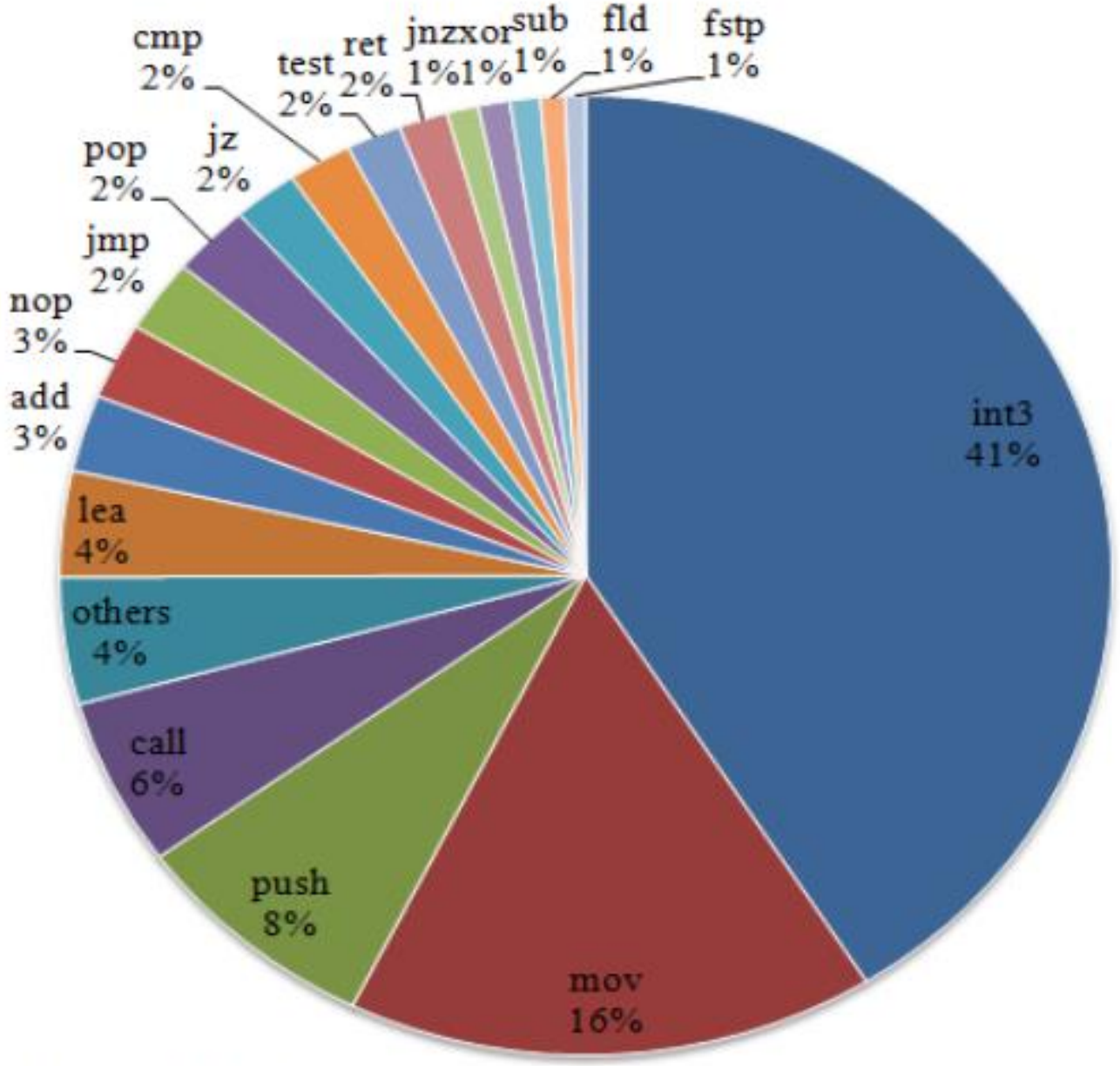


Fig. 6 Graphics Applications' instruction frequencies

Onhexgroup.ir

دستورات مهم اسمبلی

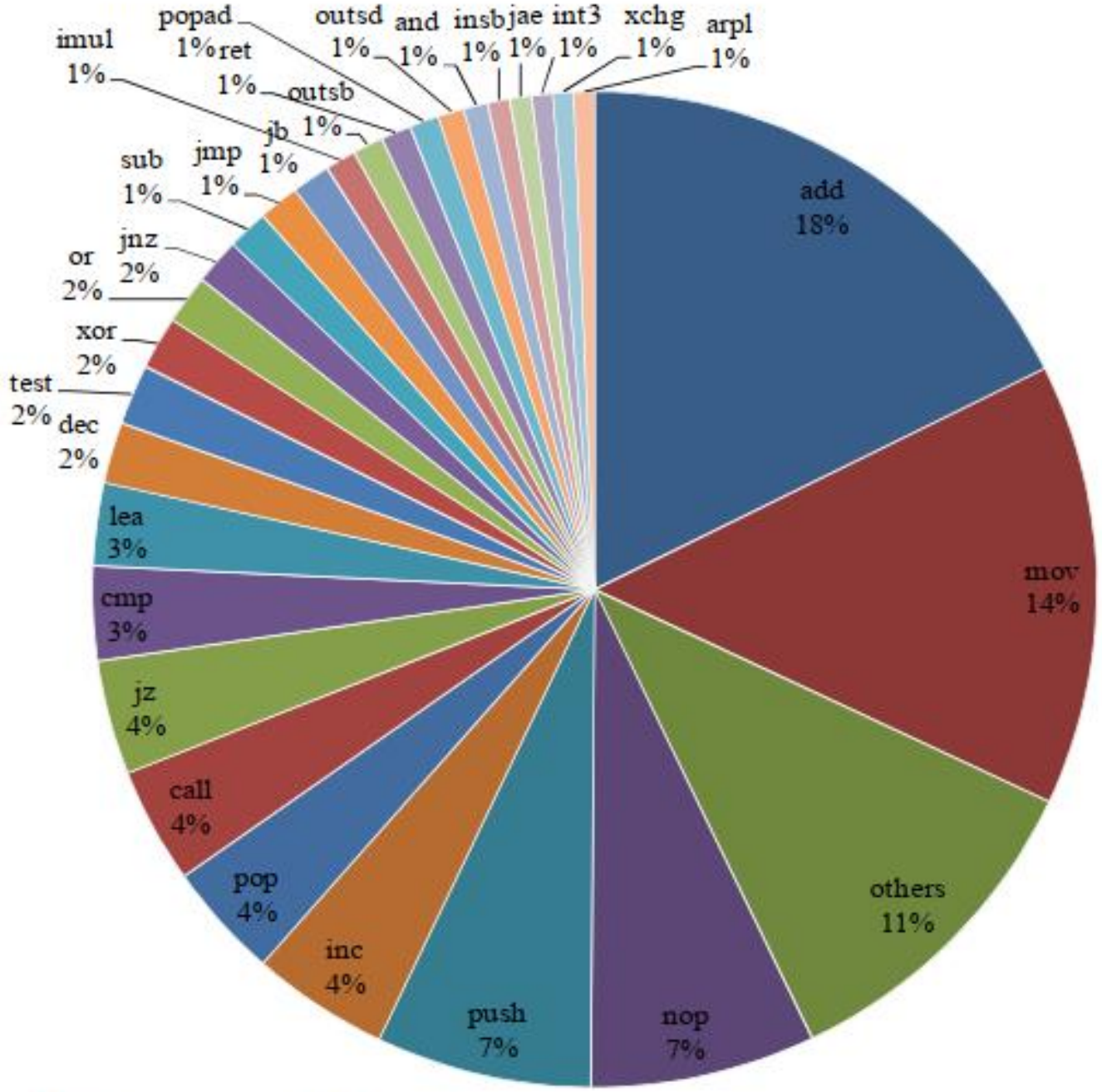


Fig. 10 OS Components' instruction frequencies.

Onhexgroup.ir

دستورات مهم اسمبلی

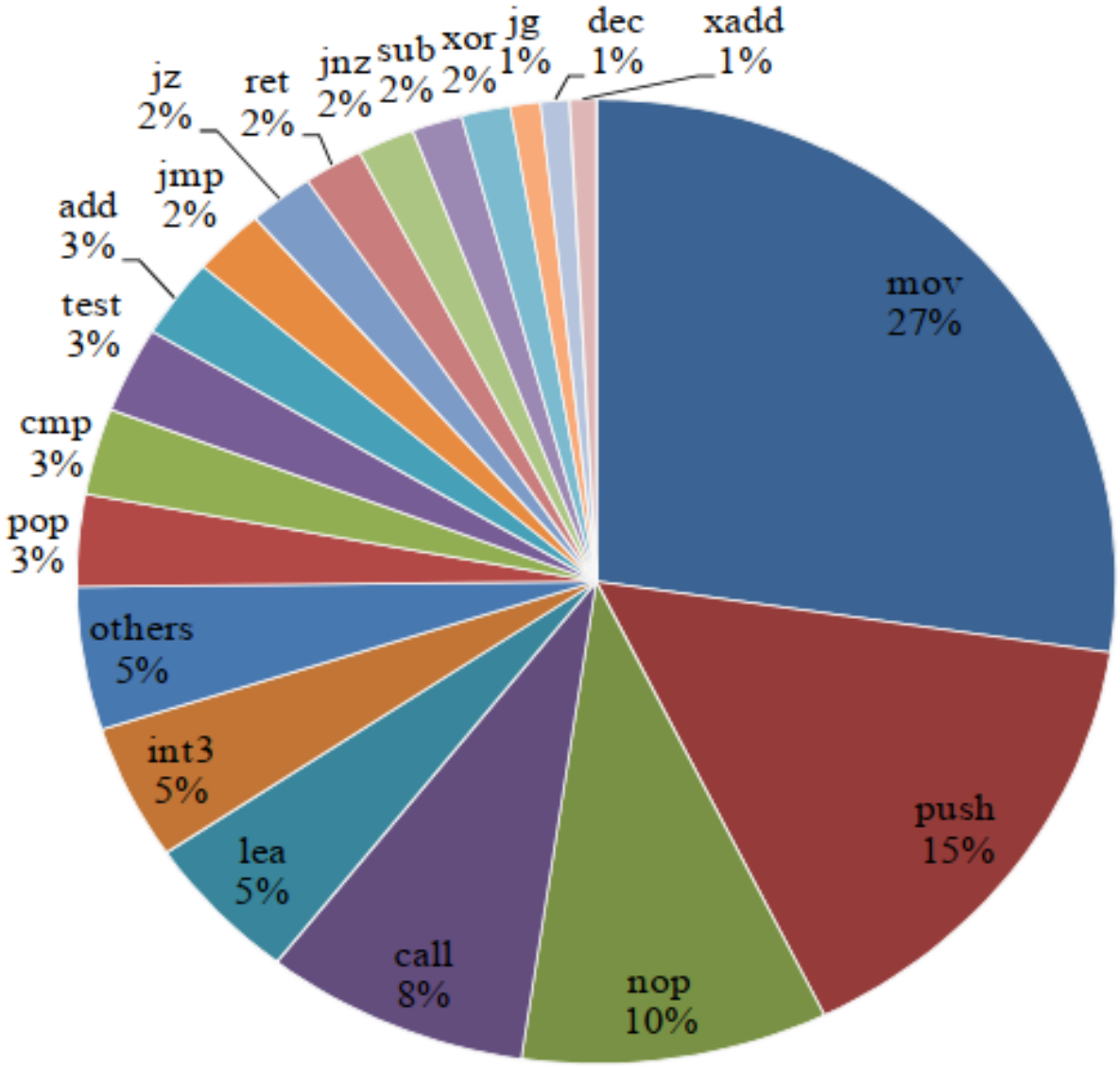


Fig. 14 General Purpose Applications' Instruction Frequencies

Onhexgroup.ir

منابع

https://en.wikipedia.org/wiki/Assembly_language

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.407.5071&rep=rep1&type=pdf