

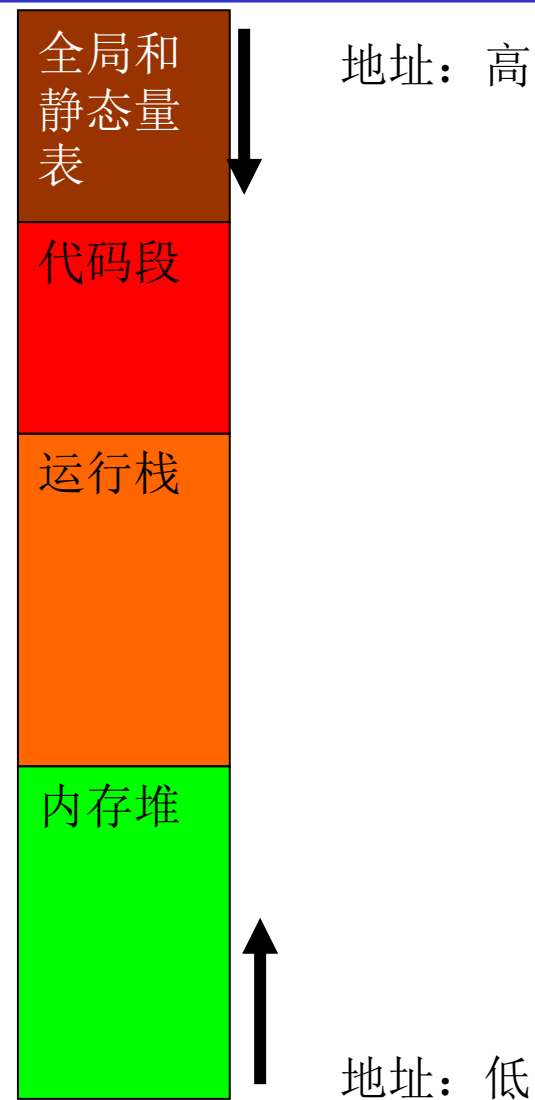
第六章 运行时的存储组织及管理

- 概述
- 静态存储分配
- 动态存储分配

运行时的存储管理

- 全局和静态量表
- 代码段
- 运行栈
- 内存堆

- 以MS-WIN+VS+X86下的可执行程序为例，从高地址到低地址，自上而下的是：
 - 全局和静态量表
 - 代码段
 - 运行栈
 - 内存堆



全局和静态量表

```
int global_c = 0 ;
```

```
void foo(int a)
```

```
{
```

```
    static int s_c = 0 ;
```

```
    s_c += a ;
```

```
    global_c = s_c ;
```

```
}
```

```
00427e34
```

```
global_c
```

```
00427e38
```

```
s_c
```

```
...
```

```
...
```

```
12:    s_c += a ;
```

```
00401028  mov     eax,[global_c+4 (00427e38)]
```

```
0040102D  add     eax,dword ptr [ebp+8]
```

```
00401030  mov     [global_c+4 (00427e38)],eax
```

```
13:
```

```
14:    global_c = s_c ;
```

```
00401035  mov     ecx,dword ptr [global_c+4 (00427e38)]
```

```
0040103B  mov     dword ptr [global_c (00427e34)],ecx
```

```
...
```

运行栈

- 子程序/函数运行时所需的基本空间
- 进入子程序/函数时分配，地址空间向下生长（从高地址到低地址）
- 从子程序/函数返回时，当前运行栈将被废弃
- 递归调用的同一个子程序/函数，每次调用都将获得独立的运行栈空间

运行栈实例分析

- 一个典型的运行栈包括
 - 函数的返回地址
 - 全局寄存器的保存区
 - 临时变量的保存区
 - 未分配到全局寄存器的局部变量的保存区
 - 其他辅助信息的保存区
 - 例，PASCAL类语言的DISPLAY区

一个XScale(ARM)上的Java/C/C++函数运行栈的示意图



```
#include <stdio.h>
#include <string.h>
void fun1( )
{
    int m=0;
    char num[4];
    strcpy(&num[12],"\x90\x10\x40\x00");
}
void fun2( ) //0x00401090
{
    printf ("You were attacked!!!\n");
}
int main()
{
    fun1();
    return 0;
}
```


6.1 概述

(1) 运行时的存储组织及管理

目标程序运行时所需存储空间的组织与管理以及源程序中变量存储空间的分配。

例: `real a, b, c ;`

...

`a := b*c ;`



取b

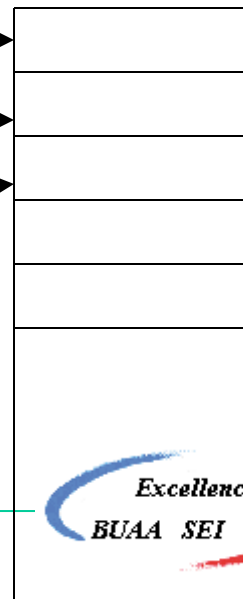
* c

送a

符号表

a	简单变量	real
b	简单变量	real
c	简单变量	real
.....		

数据区



(2) 静态存储分配和动态存储分配

静态存储分配

在编译阶段由编译程序实现对存储空间的管理和为源程序中的变量分配存储的方法。

条 件

如果在编译时能够确定源程序中变量在运行时的数据空间大小，且运行时不改变，那么就可以采用静态存储分配方法。

但是并不是所有数据空间大小都能在编译过程中确定

动态存储分配

在目标程序运行阶段由目标程序实现对存储空间的组织与管理，和为源程序中的变量分配存储的方法。

特 点

- 在目标程序运行时进行变量的存储分配。
- 编译时要生成进行动态分配的目标指令。

6.2 静态存储分配

(1) 分配策略

由于每个变量所需空间的大小在编译时已知，因此可以用简单的方法给变量分配目标地址。

- 开辟一数据区。（首地址在加载时定）
- 按编译顺序给每个模块分配存储空间。
- 在模块内部按顺序给模块的变量分配存储，一般用相对地址，所占数据区的大小由变量类型决定。
- 目标地址填入变量的符号表中。

例：有下列FORTRAN 程序段

real MAXPRN, RATE

integer IND1, IND2

real PRINT(100), YPRINT(5,100), TOTINT

假设整数占4个字节大小，
实数占8个字节大小，则
符号表中各变量在数据区中
所分配的地址为：

名字	类型	维数	地址
MAXPRN	r	0	264
RATE	r	0	272
IND1	i	0	280
IND2	i	0	284
PRINT	r	1	288
YPRINT	r	2	1088
TOTINT	r	0	5088

数据区

264

272

280

284

288

+8×100

1088

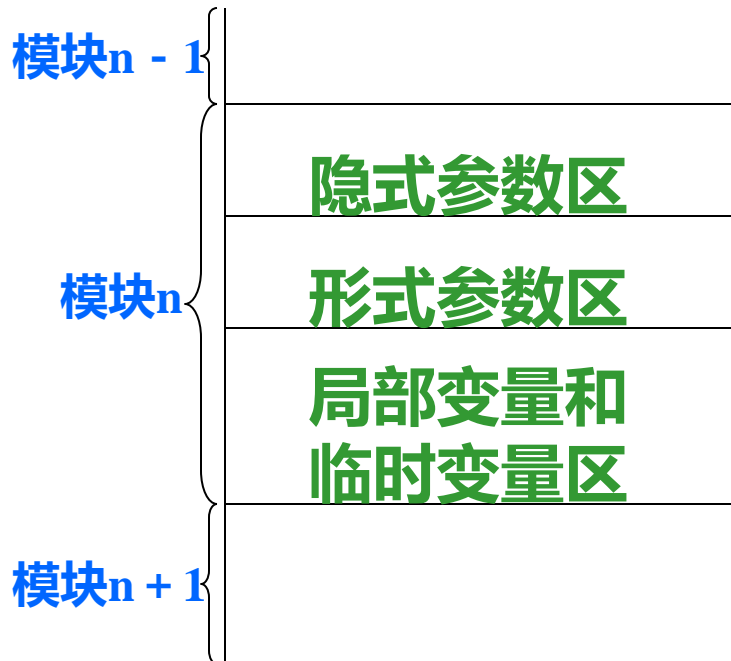
+8×100×5

5088

(2) 模块(FORTRAN子程序)的完整数据区

- 变量
- 返回地址
- 形式参数
- 临时变量

FORTRAN子程序的典型数据区



隐式参数区: 返回地址
函数返回值

形式参数区: 存放相应实参信息(值或地址)

6.3 动态存储分配

- 编译时不能具体确定程序所需数据空间
- 编译程序生成有关存储分配的目标代码
- 实际上的分配要在目标程序运行时进行

分程序结构，且允许递归调用的语言：

栈式动态存储分配

分配策略： 整个数据区为一个堆栈，

- (1) 当进入一个过程时，在栈顶为其分配一个数据区。
- (2) 退出时，撤消过程数据区。

- (1)当进入一个过程时，在栈顶为其分配一个数据区。
- (2)退出时，撤消过程数据区。

例1:

```

1  BBLOCK;
    REAL X,Y; STRING NAME;
2  M1: PBLOCK(INTEGER IND);
    INTEGER X;
    CALL M2(IND+1);
    EDN M1;
3  M2: PBLOCK(INTEGER J);
    4  BBLOCK;
        ARRAY INTEGER F(J);
        LOGICAL TEST1;
    5  END
    6  END M2;
    CALL M1(X/Y);
    8  END;
    
```

AR4 F, TEST1数据区

运行中数据区的分配情况:

AR1	X,Y,NAME数据区
-----	-------------

(a)

AR2	X和参数IND数据区
AR1	X,Y,NAME数据区

(b)

AR3	参数J
AR2	X和参数IND数据区
AR1	X,Y,NAME数据区

(c)

AR4	F, TEST1数据区
AR3	参数J
AR2	X和参数IND数据区
AR1	X,Y,NAME数据区

(d)

AR3	参数J
AR2	X和参数IND数据区
AR1	X,Y,NAME数据区

(e)

AR2	X和参数IND数据区
AR1	X,Y,NAME数据区

(f)

```

BBLOCK;
  REAL X,Y; STRING NAME;
  M1: PBLOCK(INTEGER IND);
    INTEGER X;
    CALL M2(IND+1);
  END M1;
  M2: PBLOCK(INTEGER J);
    BBLOCK;
      ARRAY INTEGER F(J);
      LOGICAL TEST1;
    END ;
  END M2;
  CALL M1(X/Y);
END
    
```

AR1	X,Y,NAME数据区
-----	-------------

(g)

6.3.1 活动记录

一个典型的活动记录可以分为三部分：

局部数据区
参数区
display区

(1) 局部数据区：

存放模块中定义的各个局部变量。

(2) 参数区： 存放隐式参数和显式参数。



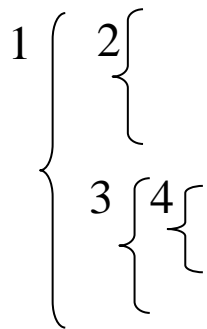
prev abp : 存放调用模块记录基地址,函数执行完时,释放其数据区, 数据区指针指向调用前的位置

ret addr: 返回地址, 即调用语句的下一条执行指令地址

ret value : 函数返回值(无值则空)

形参数据区: 每一形参都要分配数据空间,形参单元中存放实参值或者实参地址

(3) display区：存放各外层模块活动记录的基地址。



对于例1中所举的程序段，模块4可以引用模块1和模块3中所定义的变量，故在模块4的display，应包括AR1和AR3的基地址。

变量二元地址(BL、ON)

BL：变量声明所在的层次。

可得到该层数据区
开始地址

并列过程具有相同层次

ON：相对于显式参数区的开始位置的位移。

相对地址

例如：程序块1

X: (1, 0)
Y: (1, 1)
NAME: (1, 2)

过程块M1

IND: (2, 0)
X: (2, 1)

高层(内层)模块可以引用低层(外层)模块中的变量，例如在M1中可引用外层模块中定义的变量Y。

在M1的display区中可找到程序块1的活动记录基地址, 加上Y在数据区的相对地址就可以求得Y的绝对地址。

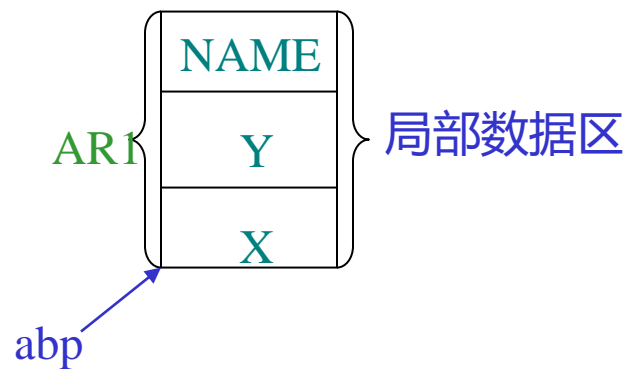
```

BBLOCK;
(1) REAL X,Y; STRING NAME;
    M1: PBLOCK(INTEGER IND);
        (2) INTEGER X;
            CALL M2(IND+1);
        END M1;
    M2: PBLOCK(INTEGER J);
        (3) BBLOCK;
            (4) ARRAY INTEGER F(J);
                LOGICAL TEST1;
            END ;
        END M2;
    CALL M1(X/Y);
END
    
```

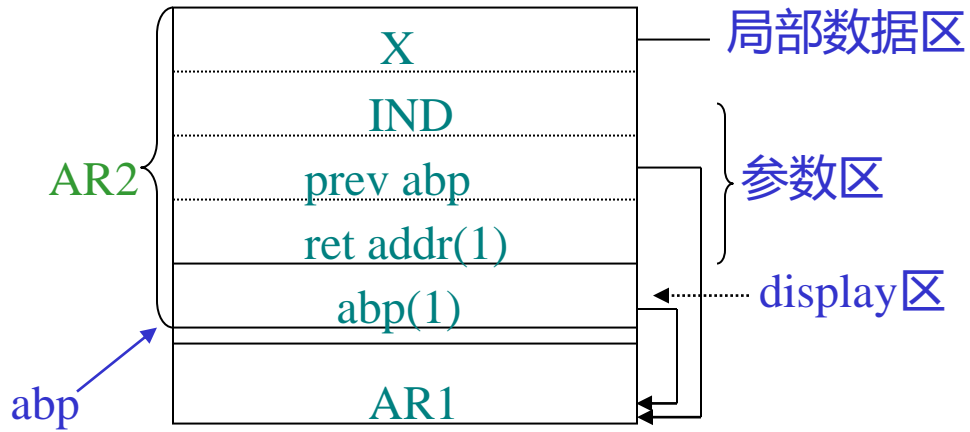
例： 下面给出上述源程序的目标程序运行时，
对运行栈(数据区栈)的跟踪情况：

```

1 { X, Y, NAME;
  2 { M1: ( IND) ;
    X;
    CALL M2;
  3 { M2: ( J);
    4 { ARRAY F(J);
      TESTI;
    CALL M1
  
```



(a) 进入模块1

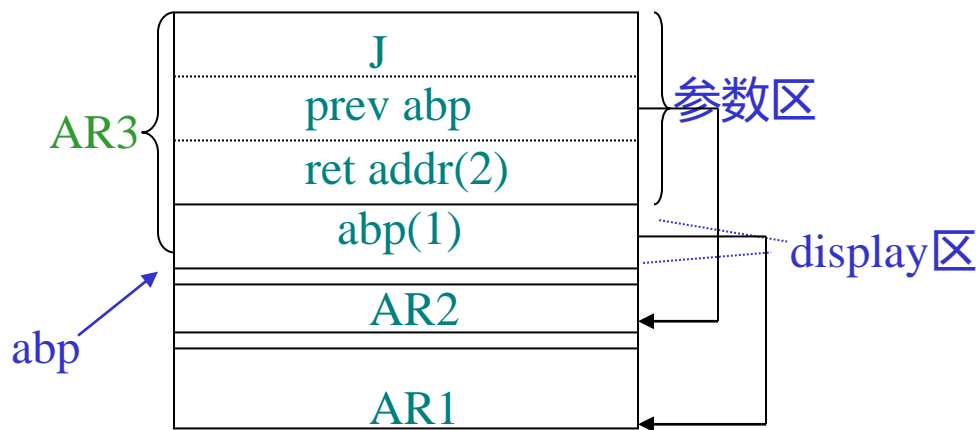


(b) M1被调用

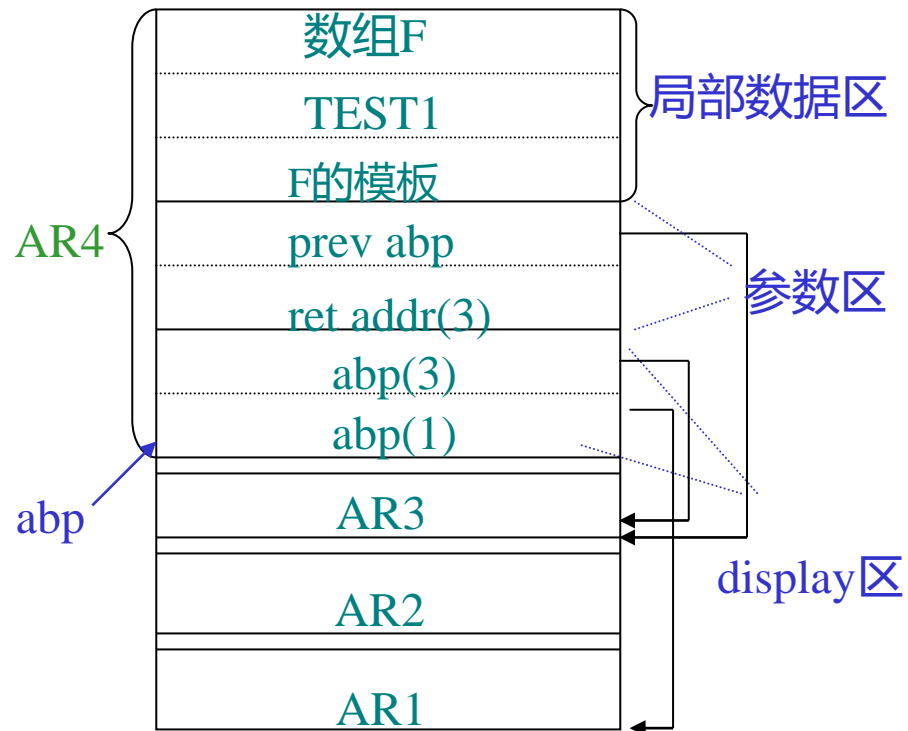
```

1 { X, Y, NAME;
  2 { M1: ( IND) ;
    X;
    CALL M2;
  3 { M2: ( J);
    4 { ARRAY F(J);
      TEST1;
    CALL M1
  }
}

```



(c) M2被调用



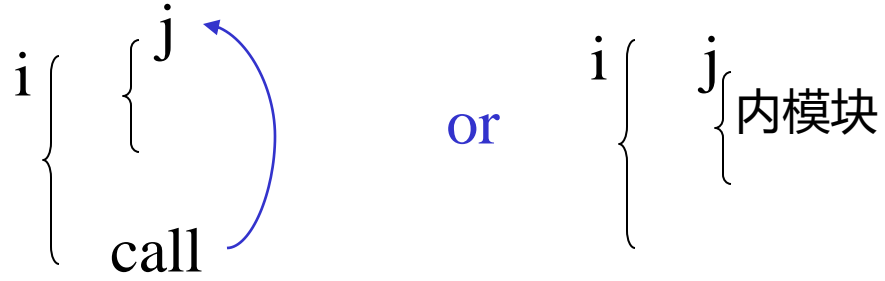
(d) 进入内模块4

- (e) 当模块4执行完, 则 $abp := prev \ abp$, 这样 abp 恢复到进入模块4时的情况, 运行栈情况如 (c)
- (f) 当M2执行完, 则 $abp := prev \ abp$, 这样 abp 恢复到进入M2时的情况, 运行栈情况如 (b)
- (g) 当M1执行完, 则 $abp := prev \ abp$, 这样 abp 恢复到进入M1时的情况, 运行栈情况如 (a)
- (h) 当最外层模块执行完, 运行栈恢复到进入模块时的情况, 运行栈空

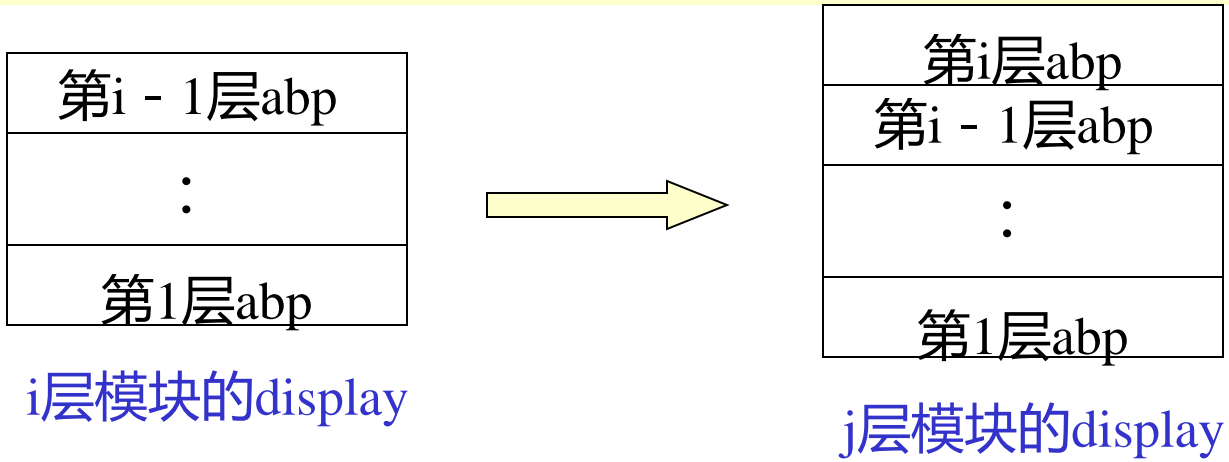
6.3.2 建造display区的规则

从i层模块进入(调用)j层模块，则：

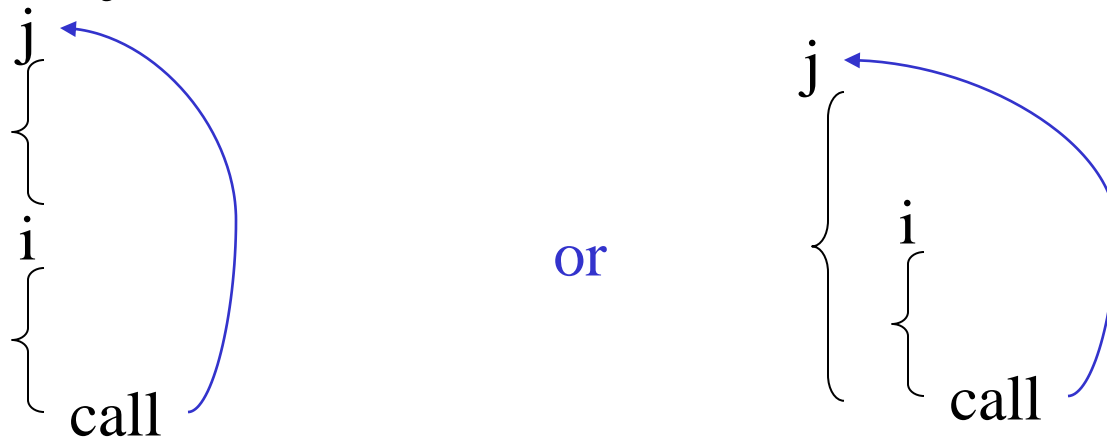
(1) 若 $j = i + 1$



复制i层的display，然后增加一个指向i层模块记录基地址的指针



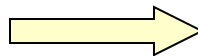
(2) 若 $j \leq i$ 即调用外层模块或同层模块



将 i 层模块的 display 区中的前面 $j - 1$ 个入口复制到第 j 层模块的 display 区

第 $i - 1$ 层 abp
第 $i - 2$ 层 abp
:
第 1 层 abp

第 i 层的 display



第 $j - 1$ 层 abp
:
第 1 层 abp

第 j 层的 display

6.3.3 运行时的地址计算

设要访问的变量的二元地址为： (BL, ON)
该变量在LEV层模块中引用

地址计算公式：

if BL = LEV then

addr := abp + (BL-1) + nip + ON

else if BL < LEV then

addr := display[BL] + (BL-1) + nip + ON

else

write(“地址错，不合法的模块层次”)

Display区大小

隐式参数区大小

作业： p133 (166) 2, 3

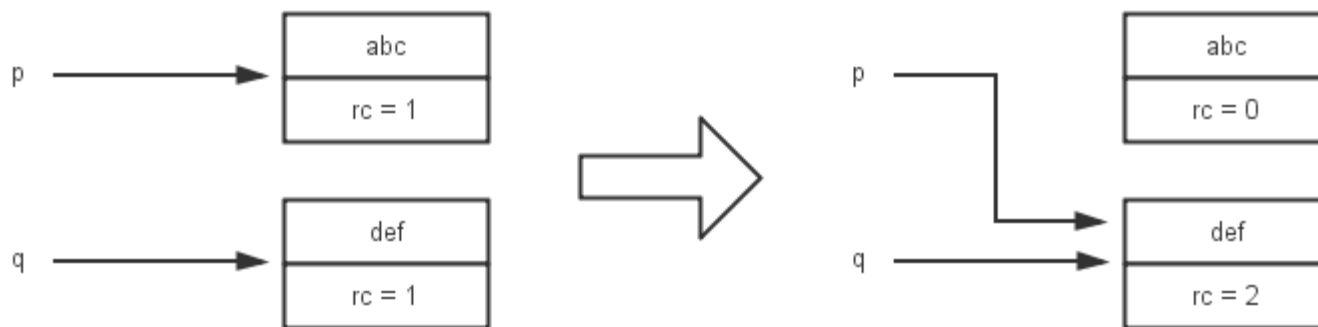
内存垃圾收集器

- 内存垃圾回收器(**Garbage Collector**, 简称**GC**)，是一种自动内存管理机制
- 第一次出现于1958年，由John McCarthy首先实现，使之作为Lisp实现的一部分
- 包括Java、JavaScript、Python、Perl、Modula-3、Prolog、ML和Smalltalk等语言的运行时系统都含有GC

GC的典型技术

- 无需标记和“stop-the-world”回收
 - 引用计数
- 需要标记和“stop-the-world”回收
 - 标记和清除
 - 标记紧缩
 - 拷贝回收
 - 分代回收

引用计数

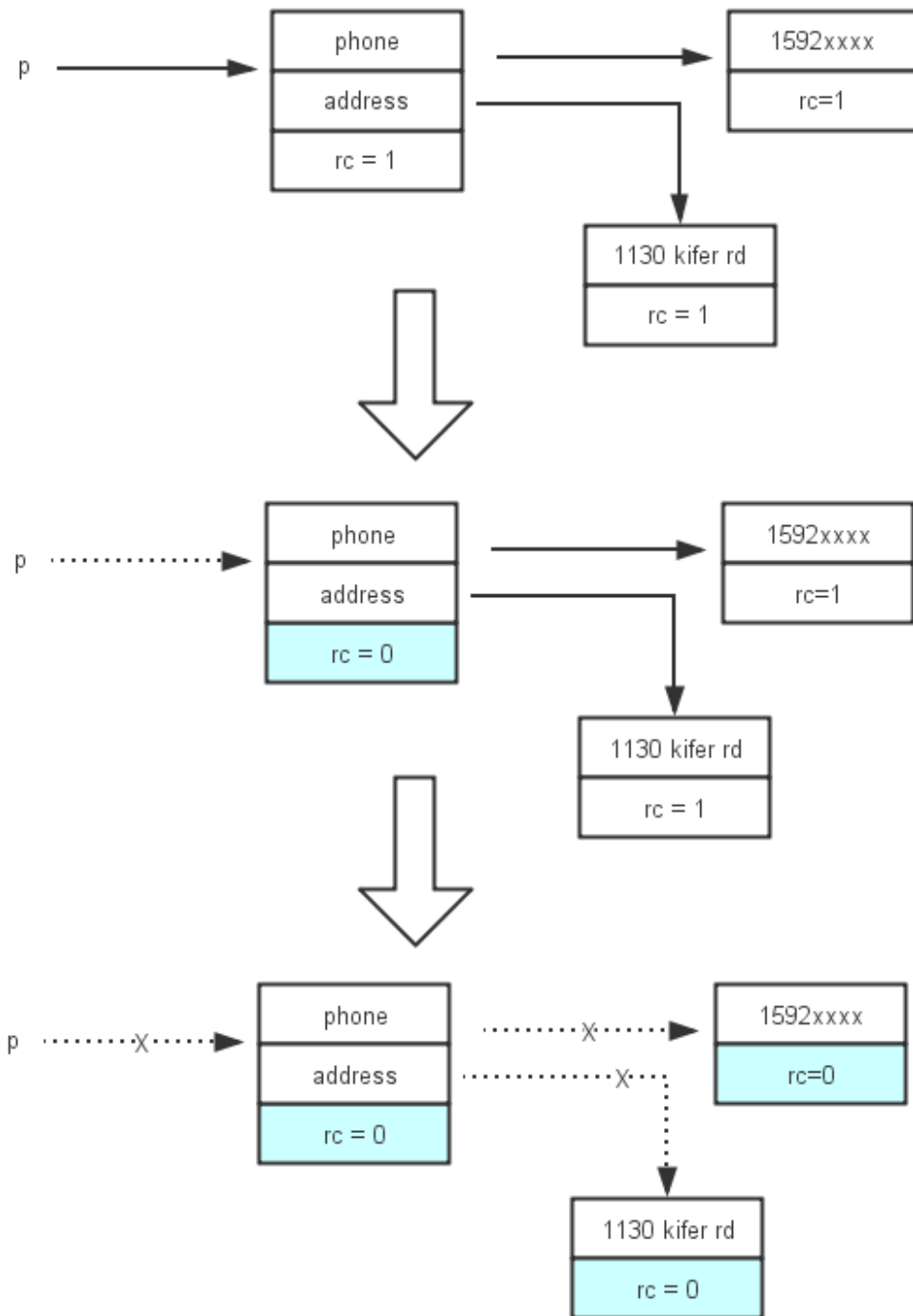


- *p*指针指向*q*的对象时，*p*原指向的对象计数减1，*q*的计数加1
- 计数减为0的对象，系统随时可以回收

引用计数的局限和问题

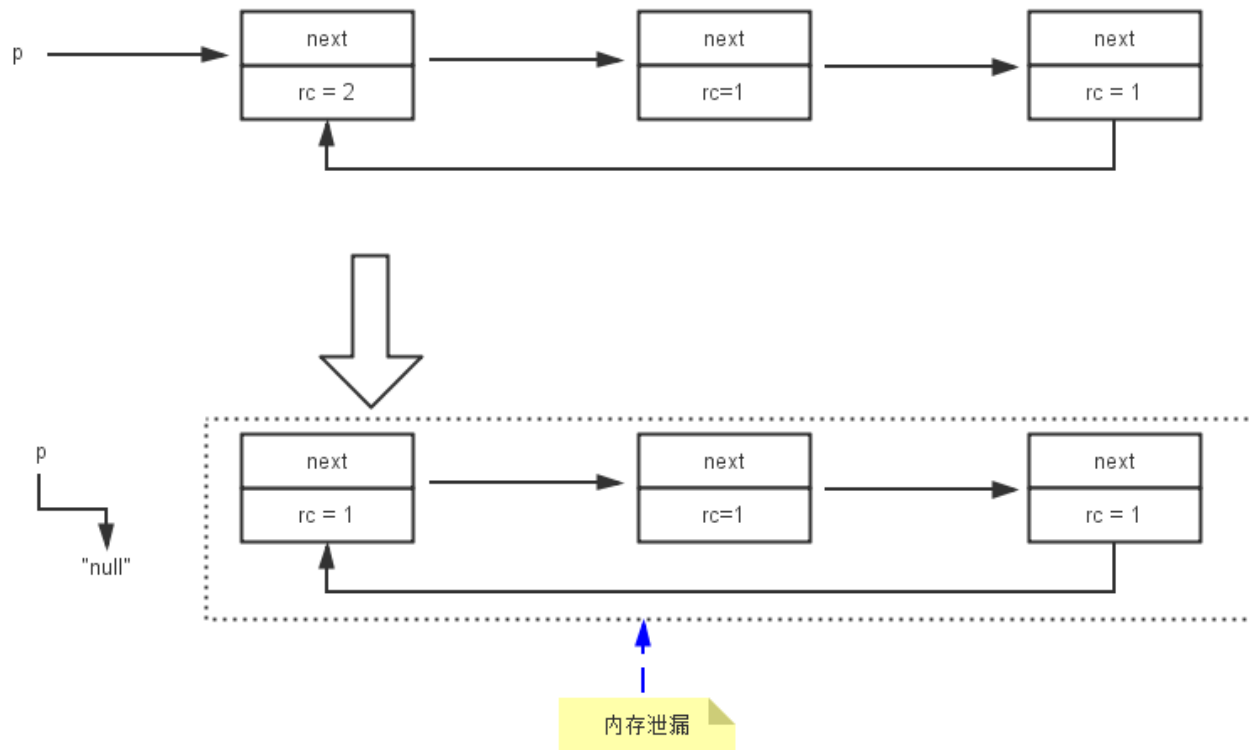
效率问题

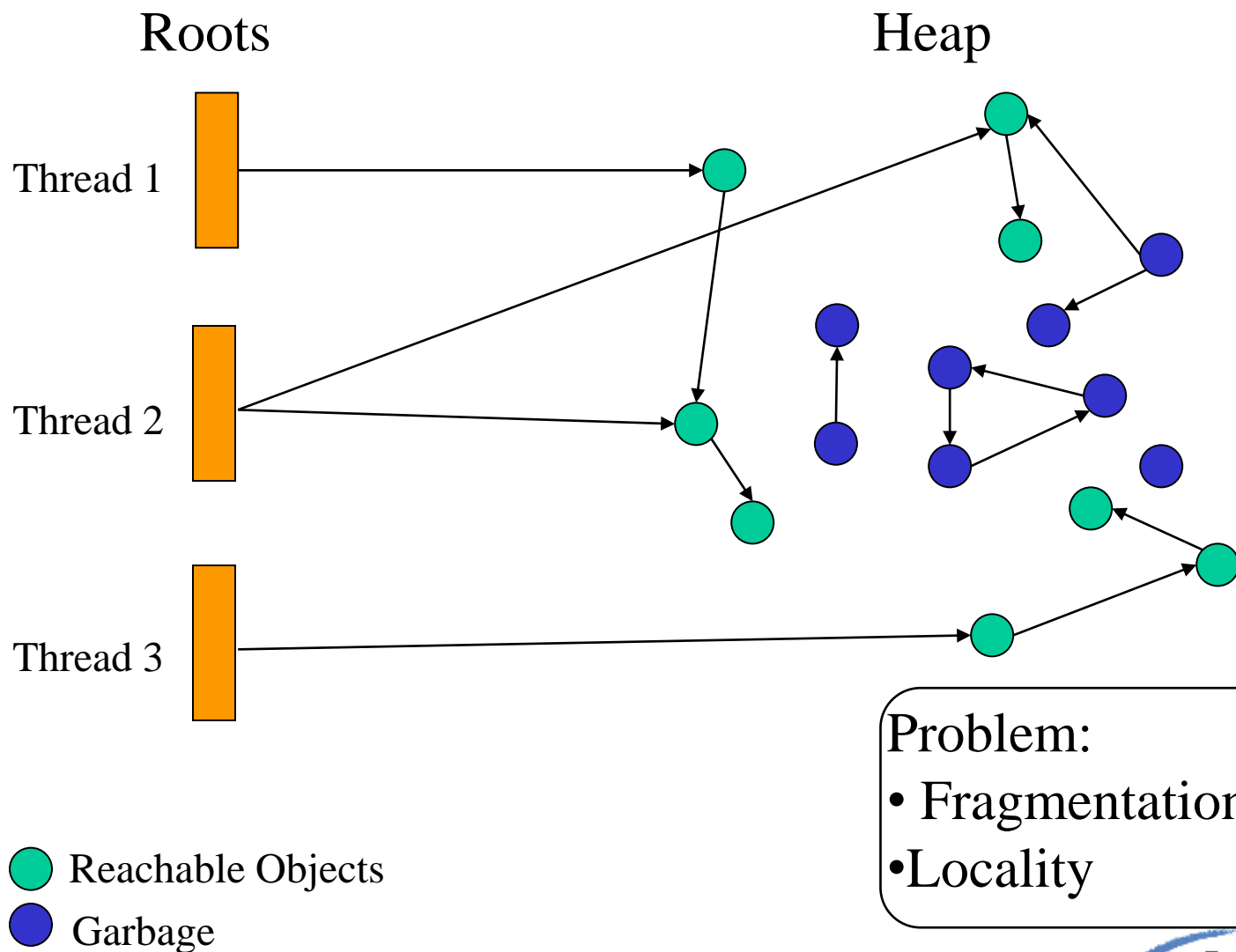
- 每次改变对象指针均需要递归改写计数（出现引用为0的情况）

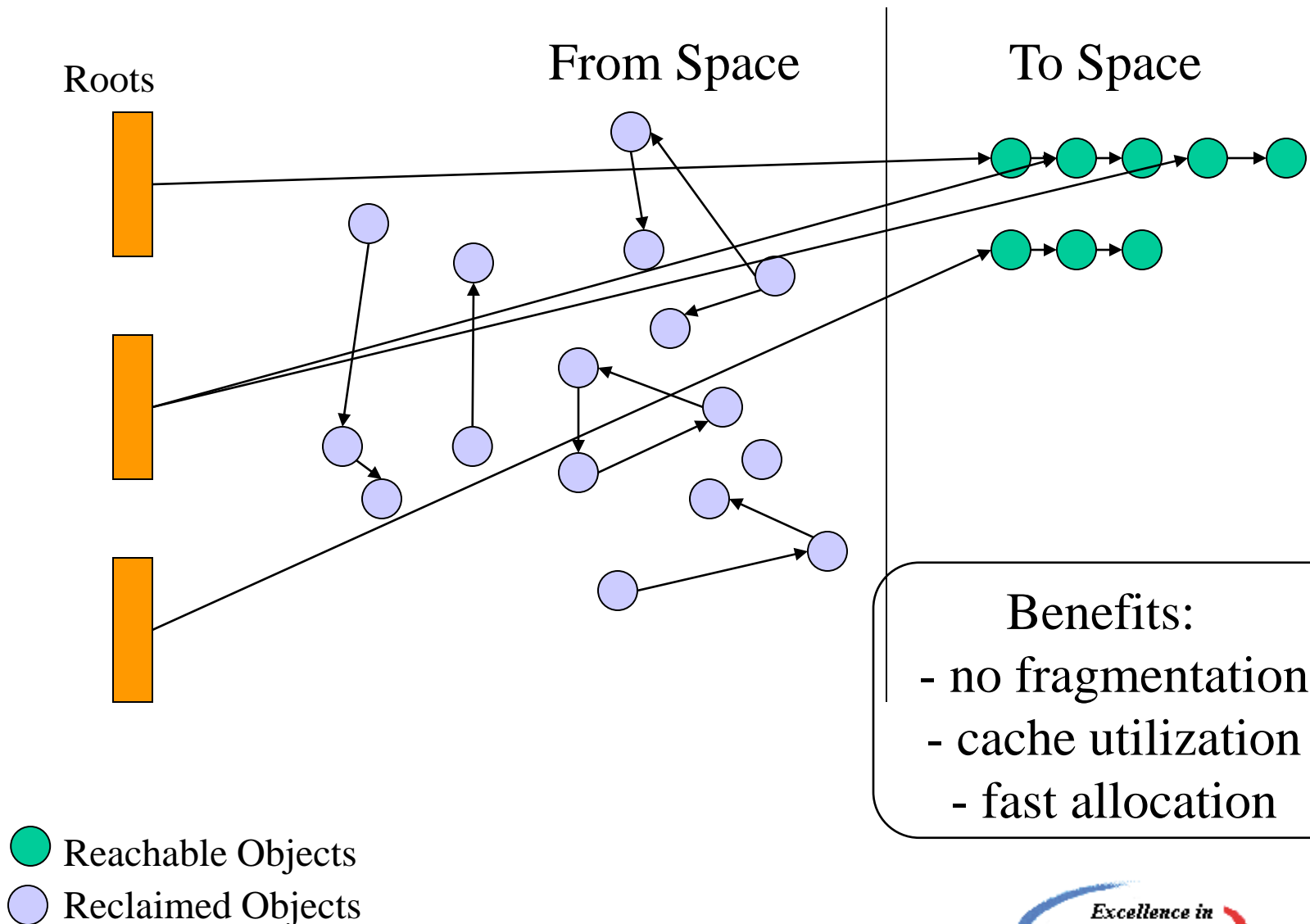


引用环问题

- 导致内存泄漏
- 通过“弱引用”解决
 - SWIFT
 - 华为方舟



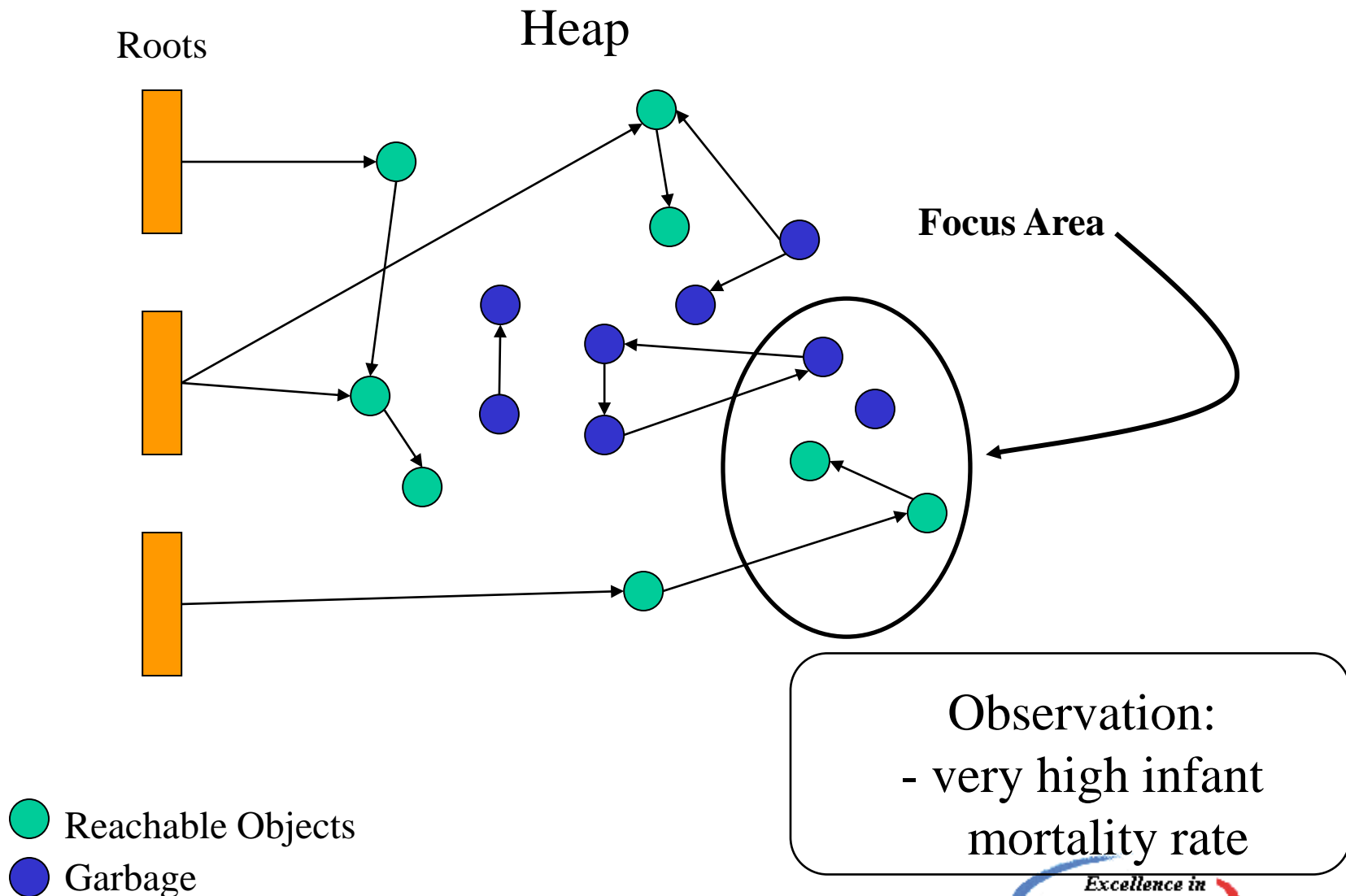




Benefits:

- no fragmentation
- cache utilization
- fast allocation

How Generational Collection works



Generational Continued

