中国科学院大学

University of Chinese Academy of Sciences

实验

2024 年 10 月 11 日

目录

1 汇编语法设计

1.1 文件分类

头文件：后缀为.fh。只能在主程序所在 f 文件包含，只能有一个.fh 文件，.fh 文件中只可以用来声明并定义变量。

f 文件：后缀为.f。可被 f 文件包含。组织如下：

```
data:
  poly evk(evknum)(dnum)(2)(L) = &"file1";
  poly p11(L) = &"file2";
  poly p12(L) = &"file3";
  ...
main proc:
  load b1 p11 0:L-1;
  load b2 p12 0:L-1;
  ...
  store res1[1] b6 0:L-1;
  call keyswitch(b8,L,0) b7 b8;
  load b5 res1[0] 0:L-1;
  load b6 res2[0] 0:L-1;
  addvv b5 b5 b7 0:L-1;
  addvv b6 b6 b8 0:L-1;
keyswitch(l,evkindex) proc:
  int dnum_now = ceil(l/dnum),i;
  intt b1 b1 0:l-1;
  ...
```

1.2 标签

可以声明和使用标记代码中不同位置的符号。目前只有两种。

1.2.1 函数名标签

函数名是可随意指定，不过函数名后需要接 proc 标签。主函数名必须是 main proc：

1.2.2 data

data 标签固定用于 f 文件开头定义局部变量。

1.3 变量

- 变量分为三种，一种是多项式变量，一种是普通整数，浮点数变量，最后一种是通用寄存器变量 (b1 ∼ b8, 为多项式寄存器，最大多项式项数为 L+K)。多项式变量会在内存中占用空间。普通变量不会分配内存空间，只用于辅助参数化编程。
- 变量如果在.fh 文件中必须在声明的同时定义。在.f 文件中可以先声明后定义。
- 最多可支持四维数组，维度大小需要在声明时指定。
- 多项式变量有两种赋值方法：1) 通过 store 指令 2) 通过指定文件，如 poly p(L) = &"datafile"。

1.4 symbolic instruction

1.4.1 类型

寄存器类型指令, 目标寄存器在前，源 1 在中，源 2 在最后.

1.4.2 指令表

还需添加三代指令

表 1: 指令表

symbol	example	description
multvv	multvv b4 b3 b2 0:ℓ+K-1	b4 = b3 * b2, 从第 1 个 limb 到第 ℓ+K 个 limb
multvs	multvs b5 b5 b1 0:L-1 0:0	b4 = b5[0:L-1] * b2[0:0], 标量向量乘，标量要扩展
intt	intt b1 b1 0:L-1	b1 逆 ntt，存回 b1
ntt	ntt b1 b1 0:L-1	同 intt
bconv	bconv b1 b2 0:K-1 0:L-1	b2 的 0 到 L-1 做 bconv 存到 b1 的 0 到 K-1。假设 bconv 的同时自动调整顺序并且把要合并的 b2 移到 b1 中, 并且假设不会占用额外资源。
mv	mv b1 b2 0:L-1	b2 移到 b1，如果 b2 项数小于 L，则补 0
addvv	同 multvv	同 multvv
addvs	同 multvs	同 multvs
subvv	同 multvv	同 multvv
subvs	同 multvs	同 multvs
load	load b1 a 0:L-1	把 a 多项式的 0 到 L-1 行 load 到 b1
store	store a b1 0:L-1	把 b10 到 L-1 行 store 到 a
pbs		
rotator		
vpu		

1.5 函数调用

- call 调用。
- 调用后则认为当前环境中通用寄存器都以改变。需在调用前用 store 保存需要的数。调用后重新 load 后使用。
- 输入参数中多项式在前,普通变量在后。输入多项式参数最多四个,到子函数中分别对应 b1,b2,b3,b4。返回多项式参数最多四个，函数调用时需指定返回寄存器。样例：call keyswitch(b8,L,0) b7,b8；