ISCAS 中国科学院软件研究所学术年会'2023
暨计算机科学国家重点实验室开放周

工具系统

映射字典导向的64位ARM到RISC-V汇编翻译

贾金成，孟鑫，朱家鑫*，唐震，王伟

* zhujiaxin@otcaix.iscas.ac.cn

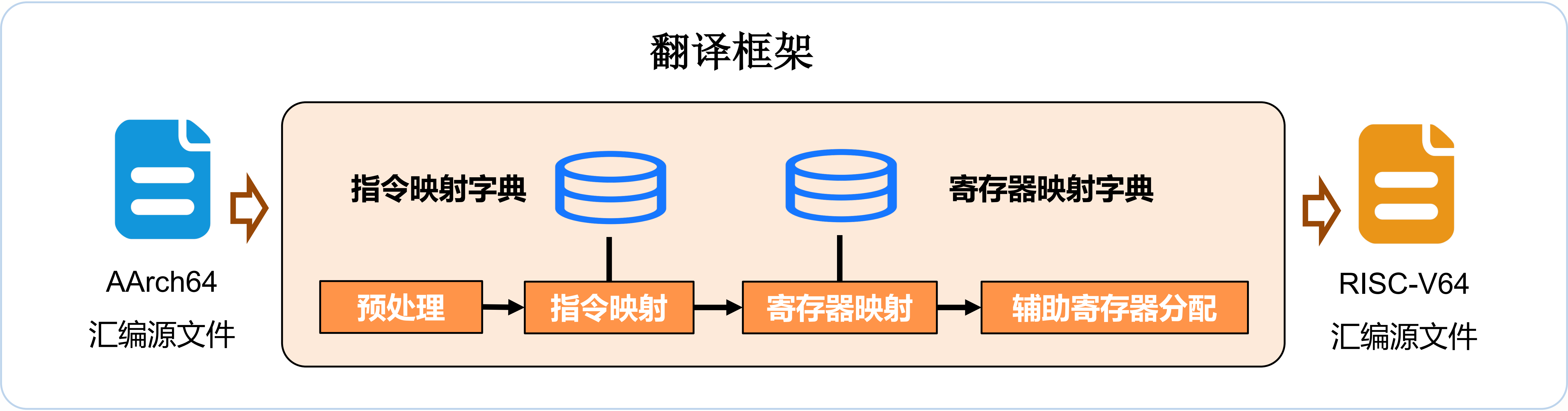
研制背景

RISC-V是一种新型开放指令集架构，近年来受到了广泛的关注。当前，RISC-V软件生态尚不完善，迁移其他成熟架构的代码是完善其生态的有效途径。汇编代码是其中基础、重要的部分，但汇编语言绑定于机器指令，相对晦涩，汇编代码迁移难度较大。

ARM 架构已经发展 30 余年，拥有完整的软件生态，特别是在嵌入式领域，积累了较多的汇编代码。

本工具面向ARM 64位指令集（AArch64）与RISC-V 64位指令集（RISC-V64），辅助开发者完成从AArch64汇编代码到RISC-V64汇编代码的迁移。

工具特性



翻译框架

AArch64
汇编源文件

指令映射字典

寄存器映射字典

预处理 → 指令映射 → 寄存器映射 → 辅助寄存器分配

RISC-V64
汇编源文件

指令映射字典

复杂指令映射字典

功能	AArch64	RiscV64
整型乘加	madd xR1,xR2,xR3,xR4	mul tR1,xR2,xR3 add xR1,tR1,xR4
立即数和32位寄存器与操作	and wR1,wR2,imm1	li tR1,imm0 and wR1,wR2,tR1

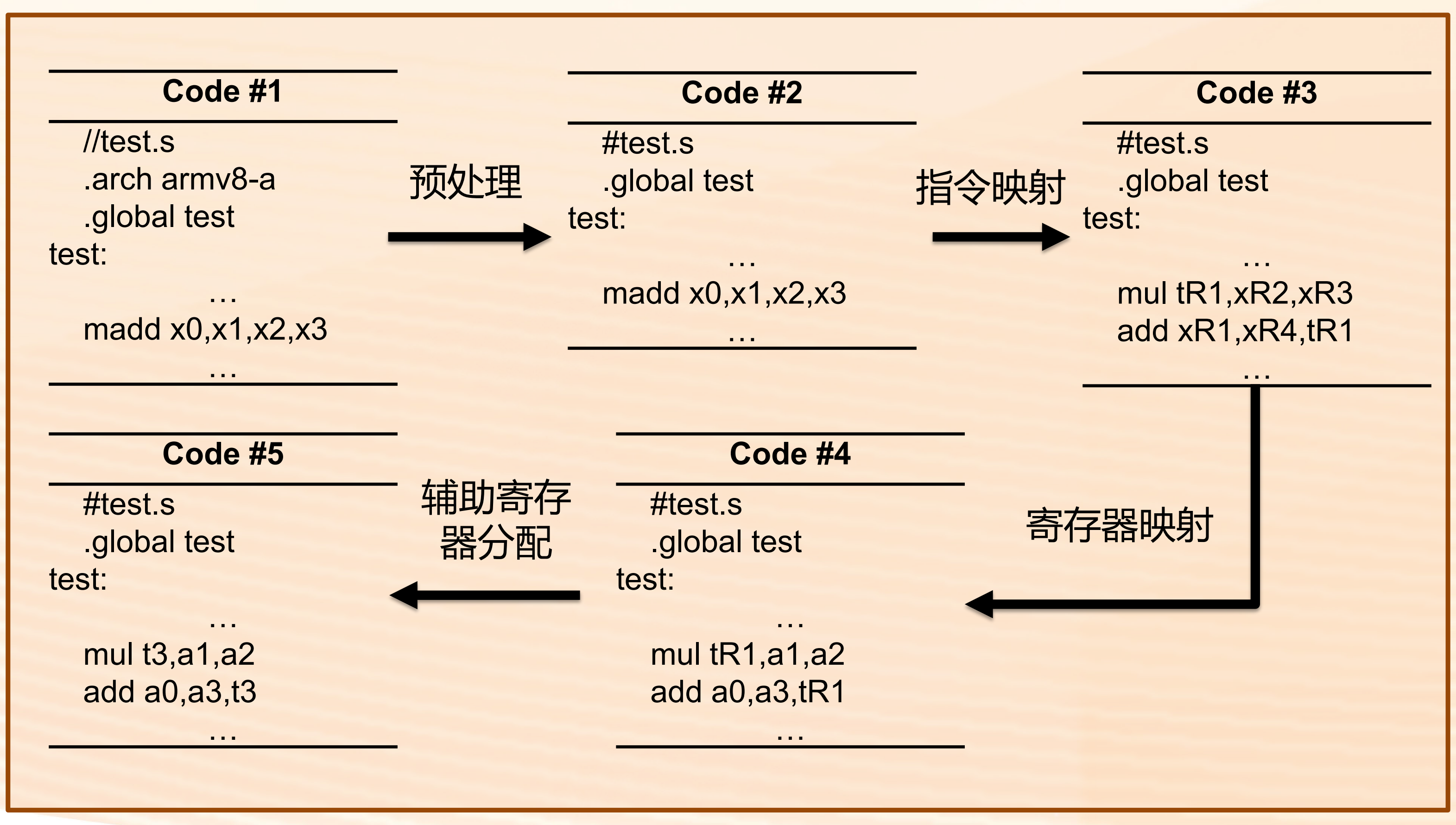
流程控制指令映射字典

AArch64	RISC-V64
cmp xR1,xR2 bge label1	bge xR1,xR2,label1
cmp xR1,xR2	neg tR1,xR2 add tR2,xR1,tR1 slti nTagR,tR2,0 sltu zTagR,x0,tR2 sltu cTagR,tR2,xR1 slti tR3,xR1,0 slt tR2,tR2,tR1 xor vTagR,tR2,tR3
bge label1	beq nTagR,vTagR,label1

寄存器映射字典

类型	AArch64	RISC-V	调用约定
寄存器直接映射	X0-X7/W0-W7	A0-A7	参数寄存器
	x9-x11/w9-w11	t0-t2	临时寄存器
	x19-x28/w19-w28	s1-s10	保存寄存器
	x29/w29	s0(fp)	帧指针寄存器
	x30/w30	Ra	返回地址寄存器
	x31	Sp	栈指针寄存器
	S0-S7/D0-D7	FA0-FA7	浮点参数寄存器
	S8-S15/D8-D15	FS0-FS7	浮点保存寄存器
	S16-S27/D16-D27	FT0-FT11	浮点临时寄存器
	S28-S31/D28-D31	FS8-FS11	——
内存模拟寄存器	x8(xr)	1	保存子程序返回地址
	x12-x15	2-5	临时寄存器
	x16-x17	6-7	子程序内部调用寄存器
	x18	8	平台寄存器

工具效果



Code #1
```
    //test.s
    .arch armv8-a
    .global test
test:
          …
    madd x0,x1,x2,x3
          …
```

预处理 →

Code #2
```
    #test.s
    .global test
test:
          …
    madd x0,x1,x2,x3
          …
```

指令映射 →

Code #3
```
    #test.s
    .global test
test:
          …
    mul tR1,xR2,xR3
    add xR1,xR4,tR1
          …
```

寄存器映射 →

Code #4
```
    #test.s
    .global test
test:
          …
    mul tR1,a1,a2
    add a0,a3,tR1
          …
```

辅助寄存器分配 →

Code #5
```
    #test.s
    .global test
test:
          …
    mul t3,a1,a2
    add a0,a3,t3
          …
```

左图展示了工具通过预处理模块、指令映射模块、寄存器映射模块和辅助寄存器模块的处理，对AArch64汇编源程序Code#1进行注释修改、指令转换和寄存器替换，最终生成RISC-V64汇编程序。