IR(Intermediate Representation)

Unknown macro: 'html'

Excuse the ads! We need some help to keep our site up. Unknown macro: 'html'

List

- IR(Intermediate Representation)
  - Intermediate language
  - Three-address code
    - Example
  - Intermediate Representation
    - QEMU TCG(Tiny code generator)
    - Valgrind VEX
      - Example
    - LLVM(Low Level Virtual Machine) IR:
      - Example
  - Related info

IR(Intermediate Representation)

- IR(Intermediate Representation) .
- IR .
- IR IR , , .
- IR .
  -
  - (,Intermediate language)

Intermediate language

- .
- .
- 3 .
  - .
  - .
  - .
- Three-address code(TAC or 3AC) .

> **(Abstract machine)**
>
> - , .

Three-address code

- Three-address code TAC 3AC .
- TAC (intermediate code) .
- TAC .
- TAC , .

Example

- "x = (a + b * c) / 2" .

x = (a + b * c) / 2

```
t1 := b * c
t2 := a + t1
t3 := t2 / 2
x := t3
```

- .

Sample code

```
for(i = 0; i < 100; i++){
        val[i] = i;
}
```

Three-address code

```
     t1 := 0
L1:  if t1 >= 100 goto L2
     t2 := t1 * 4
     t3 := val + t2
     *t3 := t1
     t1 := t1 + 1
     goto L1
L2:
```

Intermediate Representation

QEMU TCG(Tiny code generator)

- TCG QEMU TCG IR(Intermediate Representation) .
- TCG TCL .
- QEME
  - arm, i386, ia64, ppc, ppc64, s390, sparc, x86_64

TCG Readme

- https://git.qemu.org/?p=qemu.git;a=blob_plain;f=tcg/README;hb=HEAD
- http://repo.or.cz/w/qemu/ar7.git/blob_plain/HEAD:/tcg/tci/README

Valgrind VEX

- VEX TCG , .
- VEX IR .
  - Expressions
  - Operations
  - Temporary variables.
  - Statements
  - Blocks

Example

- .

The following ARM instruction

```
subs R2, R2, #8
```

Becomes this VEX IR

```
t0 = GET:I32(16)
t1 = 0x8:I32
t3 = Sub32(t0,t1)
PUT(16) = t3
PUT(68) = 0x59FC8:I32
```

- https://docs.angr.io/docs/ir.html

LLVM(Low Level Virtual Machine) IR:

- LLVM IR Low-level .
- LLVM IR % .
- LLVM .
  - C IR
  - IR
  -

Example

- IR .

Install the llvm

```
$ sudo aptitude install llvm clang
```

Sample code

```
int sample(int a,int b) {
            return a*b;
}
```

Create the llvm IR

```
lazenca0x0@ubuntu:~$ cat sample.ll
; ModuleID = 'test.c'
target datalayout = "e-m:e-i64:64-f80:128-n8:16:32:64-S128"
target triple = "x86_64-pc-linux-gnu"

; Function Attrs: norecurse nounwind optsize readnone uwtable
define i32 @sample(i32 %a, i32 %b) #0 {
  %1 = mul nsw i32 %b, %a
  ret i32 %1
}

attributes #0 = { norecurse nounwind optsize readnone uwtable "disable-tail-calls"="false" "less-precise-fpmad"
="false" "no-frame-pointer-elim"="false" "no-infs-fp-math"="false" "no-nans-fp-math"="false" "stack-protector-
buffer-size"="8" "target-cpu"="x86-64" "target-features"="+fxsr,+mmx,+sse,+sse2" "unsafe-fp-math"="false" "use-
soft-float"="false" }

!llvm.ident = !{!0}

!0 = !{!"clang version 3.8.0-2ubuntu4 (tags/RELEASE_380/final)"}
lazenca0x0@ubuntu:~$
```

Related info

- https://en.wikipedia.org/wiki/Intermediate_representation
- https://wiki.qemu.org/Documentation/TCG
- http://repo.or.cz/w/qemu/ar7.git/blob_plain/HEAD:/tcg/tci/README
- https://en.wikipedia.org/wiki/Three-address_code

Unknown macro: 'html'