( ),2015,46(4):621-624 VOL.46 NO.4 2015
Journal of Shandong Agricultural University (Natural Science Edition) doi:10.3969/j.issn.1000-2324.2015.04.029

数理逻辑的程序可靠性验证

顾名宇
, 561000

摘 要:
SPIN

关键词: ; ;
中图法分类号: TP301 **文献标识码:** A **文章编号:** 1000-2324(2015)04-0621-04

Validation of Reliability on Mathematical Logic Program

GU Ming-yu
561000,

Abstract: The reliability verification of program often takes a very long time to develope the software, while the current software reliability verification method is mainly based on formal methods such as SPIN based on model checking method, but this method may lead to the complexity of verification to improve greatly bing due to model problems, and then finally fails in validation results everywhere. In order to solve this problem, this paper used mathematical methods from mathematical logic perspective to realize the program reliability verification, and completed the reliability verification of client server program, the method was be proved the validity in true.

Keywords: Mathematical logic; program; validation

,
SPIN [2][6]

100% 90% 70%
,
,

1 数理逻辑

[5] 1847

“ ” “ ”

1.1 命题演算

“ ”

收稿日期: 2013-07-13 **修回日期:** 2013-07-24
作者简介: (1960-), , , . : , . E-mail:gumingyu60@126.com

x==0,

y=5;

P: “x==0”

Q: “y=5”

“ x==0, y=5” P->Q

1.2 谓词演算

x==0, y=5 P(x,y) x==y,Q(x,y) x=y,x y

P(x,0)->Q(y,5)

2 使用数理逻辑验证程序可靠性方法

2.1 程序可靠性定义

IEEE

“ ”

1

2

2.2 程序可靠性验证步骤

1 [5] [3]

x1,x2,x3,…,xn n

V(xi)(0<=i<=n) xi F1,F2,…Fm ,

P1,P2,…PK S

y1,y2,…yl W(yj) yj , 0<=j<=l,

2

∨ ∨ ∨

∧ ∧

S

0<=l<=n,0<=t<=n

T “ ”

3

[1]

S

3 用数理逻辑法验证客户服务器程序

R1..Rn

R1……Rn

R_Work[Max] Max R_Work[i].bz = 0 (0<= i < Max)

R_Work[Max] F1

```
for (int i = 0; i < Max; i++)
{
if(R_Work[i].bz == 0)
{

break
}
}
```

F2

```
for  int j = 0  j < Max; j++
{
if(R_Work[j].bz != 0)
{

R_Work[j].bz = 0
break
}
}
```

F1 F2 F1 1-MAX F2

i R_Work[i].bz = 0 F1(i),0<=i<MAX

i j R_Work[j].bz != 0 F2(j) 0<=j<MAX

j

i F1(i), j F2(j)

R_Work[i].bz = 0 F1(i)

R_Work[j].bz != 0 F2(j)

i<j R_Work[i].bz = 0 F1(i) F2(i) F1(i)->T F2(j)->T i==j

F1 F2 F2

F1 F2 R_Work[i]
R_Work Max*log Max

R_Nextwork (0) F1 F2

```
程序 F3:
int k;
for (int i = 0; i < Max; i++)
{
k = (R_Nextwork+ i) % Max;
if (R_Work [k] .bz == 0)
{
提交任务
break
}
}
```

```
程序 F4:
int k
For (int i =0;  i <Max; i++)
{
= (R_Nextwork+ j )% Max;
(R_Work[k].bz!= 0)

执行任务
_Work[k].bz = 0;
_Nextwork= (k +1) % Max;
reak;
}
}
```

[4] F1 F2

R1,….,Rn, Ri Rk Ri<Rk
F3(Ri)->T F3(Rk)->T F4(Rk)->T
F4(Ri) F4(Rk) , F4(Ri)->T

1 F3 F3(Ri)->T F3(Rk)->T Ri<Rk Ri Rk
2 F4 F4(Rk)->T F4(Rk) Ri R_Nextpoll = Ri k k = (R_Nextpoll + i)%Max i> 0 Rk Ri Rk k

1 2 Ri Rk , F4(Rk)->T F4(Ri)->T F4(Rk)

4 小 结

参考文献

[1] . [J]. ,2014,40(2):86-91,96
[2] , , , . SPIN [J]. ,2011,33(4):902-907
[3] Alexey G, Honseok Y. Modular Verification of Preemptive OSKernels[J]. ACM SIGPLAN Notices,2011,46(9):404-417
[4] Cohen E, Schulte W, Tobies S. Local Verification of Global Invariants in Concurrent Programs[C]//Proceedings of the 22nd international conference on Computer Aided Verification.Berlin:Springer 2010:480-494
[5] , . [J]. ,2009,20(8):2051-2061
[6] , . SPIN CSCW [J]. ,2008,18(4):9-12,15
[7] 0'Heam P W. Tutorial on Separation Logic[C]//Proeeedings of the 20th International Conference on Computer Aided Verification.Berlin: Springer, 2008:15-21