



浙江大学
ZHEJIANG UNIVERSITY

基于符号抽象的程序分析

rainoftime
rainoftime.github.io
pyaoaa@zju.edu.cn

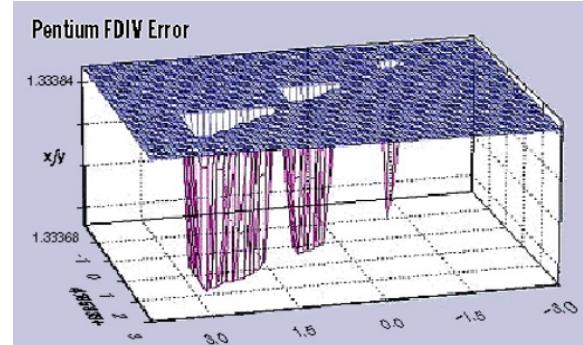
保障软件质量的重要性



数值溢出漏洞导致Ariane5火箭升空数秒后爆炸



软件漏洞导致美国东北部大面积停电



Intel Pentium漏洞导致声誉和巨额经济损失



软件漏洞导致丰田回收120万辆Prius汽车



纳斯达克OMX系统发生故障造成1300 万美元损失



软件漏洞导致放疗仪使用超过量的放射物

程序分析: 保障软件质量的重要手段

静态分析



动态分析



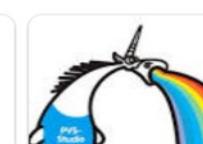
SonarQube



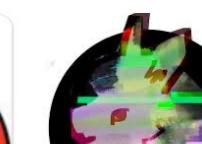
Coverity



Cppcheck



PVS-Studio



AEL++



...



抽象解释理论

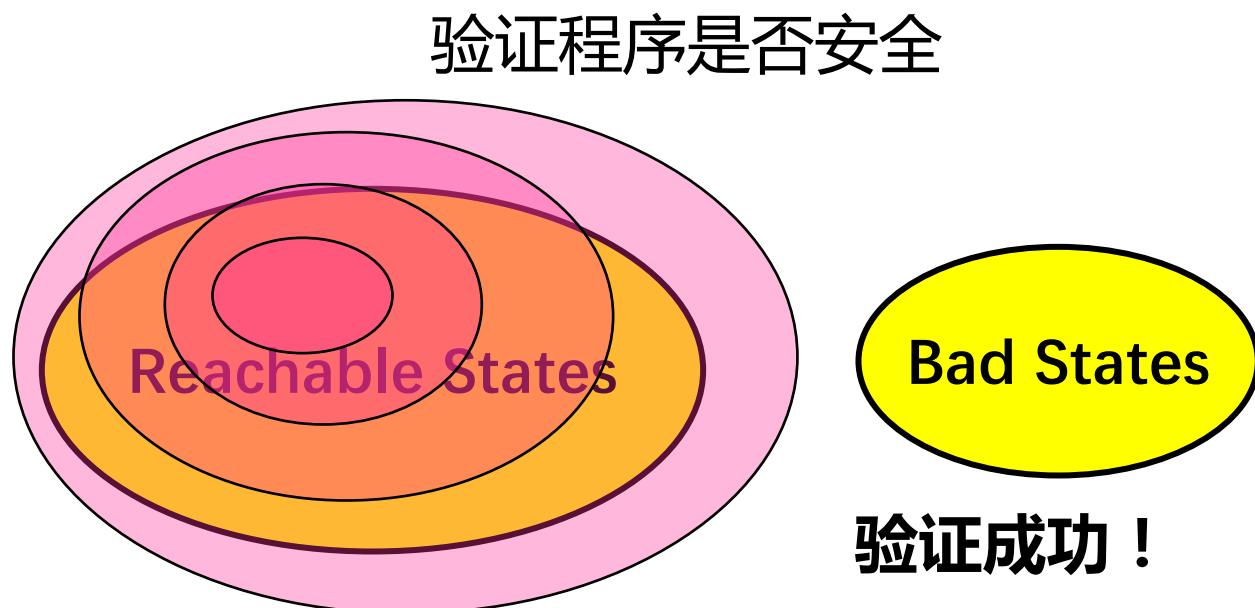
符号抽象框架

个人近期工作

一些相关问题

抽象解释(Abstract Interpretation)

- 静态程序分析的核心理论 [Cousot & Cousot, POPL'77]
- 对程序的可达状态做上近似



ABSTRACT INTERPRETATION : A UNIFIED LATTICE MODEL FOR STATIC ANALYSIS
OF PROGRAMS BY CONSTRUCTION OR APPROXIMATION OF FIXPOINTS

Patrick Cousot^{*} and Radhia Cousot^{**} @ POPL 1977

抽象解释的一些应用

- 1996~ : 涌现了多个基于抽象解释的程序分析与验证工具

Astrée

数值分析



空中客车A340主飞控软件
(13.2万行C 代码)

TVLA

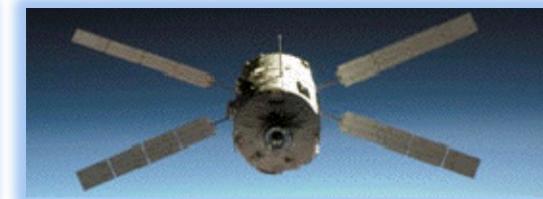
形态分析



空中客车A380主飞控软件
(约35万行C 代码)

CodeSurfer/x86

二进制分析



欧空局自动货运飞船ATV “儒勒
凡尔纳” 号 (约19万行C 代码)



抽象解释的一些应用

- 1996~ : 涌现了多个基于抽象解释的程序分析与验证工具

Astrée

数值分析

TVLA

形态分析

CodeSurfer/x86

二进制分析

与分离逻辑分庭抗礼 → “收编”基于分离逻辑的静态分析



抽象解释的一些应用

- 1996~ : 涌现了多个基于抽象解释的程序分析与验证工具

Astrée

数值分析

TVLA

形态分析

CodeSurfer/x86

二进制分析

*Value-Set Analysis(值集分析)*已成为二进制分析框架标配

BitBlaze

BAP

angr

BINSEC



抽象解释所获部分荣誉

- 2013: SIGPLAN程序语言成就奖

SIGPLAN
To explore programming language concepts and tools focusing on design, implementation and efficient use.

RECENT NEWS VIRTUAL SIG

Home Awards Conferences Resources Membership SIGPLAN Research Highlights Student Information Publications Announcements

Programming Languages Achievement Award

Given by ACM SIGPLAN to recognize an individual or individuals who has made a significant and lasting contribution to the field of programming languages. The contribution can be a single event or a life-time of achievement. The award includes a prize of \$5,000. The award is presented at SIGPLAN's PLDI conference the following June.

Nominations

- Details of the nomination and award process ([pdf](#)).
- Please use <http://awards.sigplan.org/> to submit nominations.

Recipients of the Achievement Award

2013: Patrick and Radhia Cousot

Patrick and Radhia Cousot are the co-inventors of abstract interpretation, a unifying theory of sound abstraction and approximation of structures involved in various domains of computer science, such as formal semantics, specification, proof, and verification. In particular, abstract interpretation has had a major impact on the development of the static analysis of software. In their original work, the Cousots showed how to relate a static analysis to a language's standard semantics by means of a second, abstract semantics that makes precise which features of the full language are being modeled and which are being discarded (or abstracted), providing for the first time both a formal definition of and clear methodology for designing and proving the correctness of static analyses. Subsequently, the Cousots contributed many of the building blocks of abstract interpretation in use today, including chaotic iteration, widening, narrowing, combinations of abstractions, and a number of widely used abstract domains. This work has developed a remarkable set of intellectual tools and has found its way into practice in the form of widely used libraries and frameworks. Finally, the Cousots and their collaborators have contributed to demonstrating the utility of static analysis to society. They led the development of the Astrée static analyzer, which is used in the medical, automotive, and aerospace industry for verifying the absence of a large class of common programming errors in low-level embedded systems code. This achievement stands as one of the most substantial successes of program verification to date.

- 2018: 约翰·冯诺依曼奖



Patrick Cousot awarded
John von Neumann
Medal

Patrick Cousot is the recipient of the IEEE John von Neumann medal, given "for outstanding achievements in computer-related science and technology".

[Read More](#)

◀ ▶

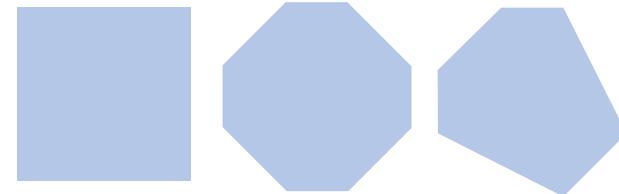
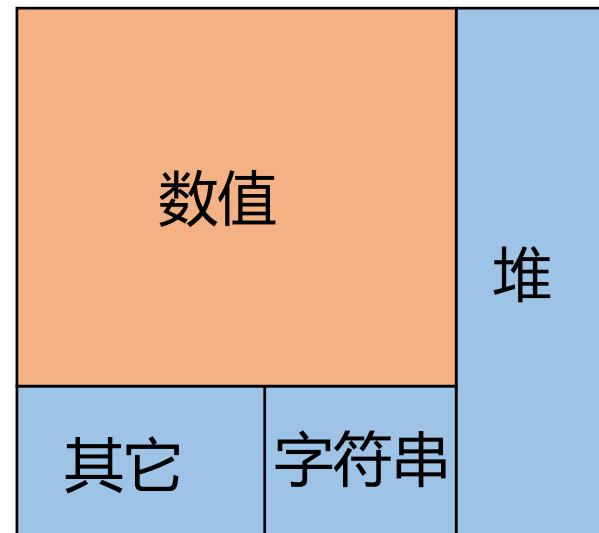
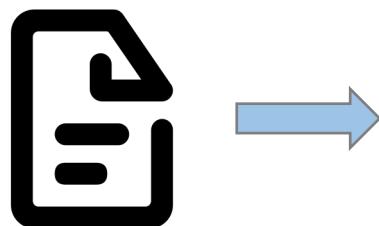
IEEE JOHN VON NEUMANN MEDAL RECIPIENTS

2018 PATRICK COUSOT
Professor, New York University,
New York, New York, USA

"For introducing abstract interpretation, a powerful framework for automatically calculating program properties with broad application to verification and optimization."

抽象域及其要素

- 对程序语义的一种数学近似

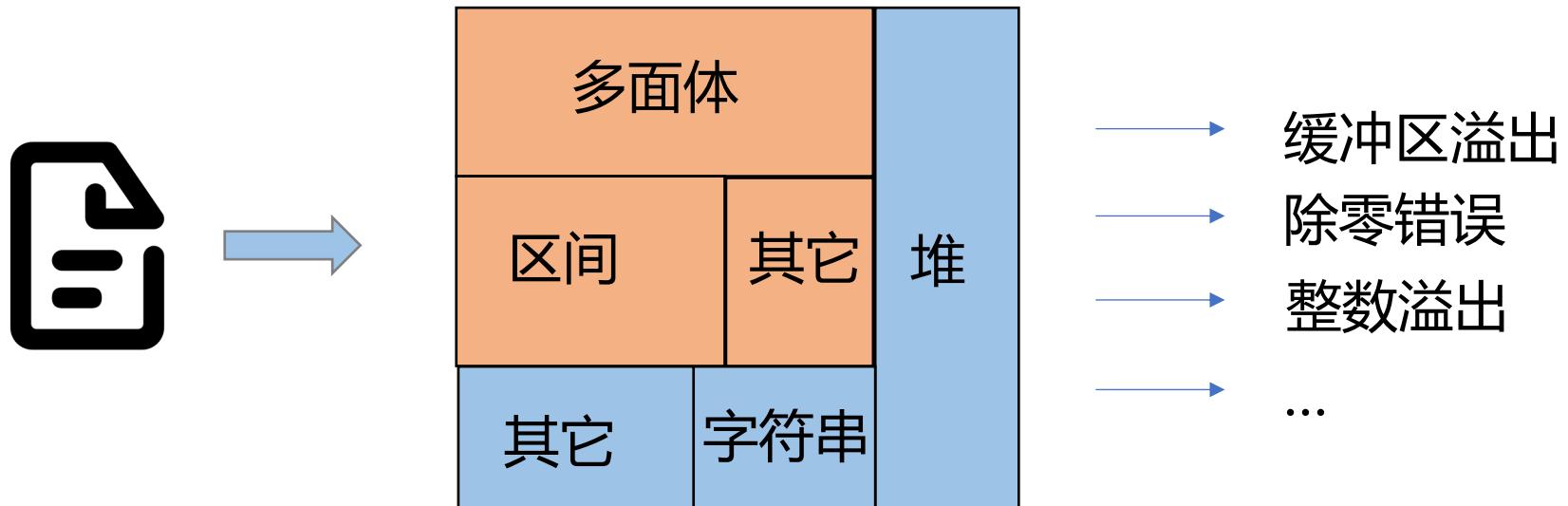


抽象元素
“程序的状态是什么”

$$M \sqcap \sqsubseteq \nabla$$
$$[x := e] \quad [x < e]$$

抽象迁移函数
“状态是怎么变迁的”

- 捕捉程序数值相关的属性



抽象域

区间域 [Cousot & Cousot, POPL'77]

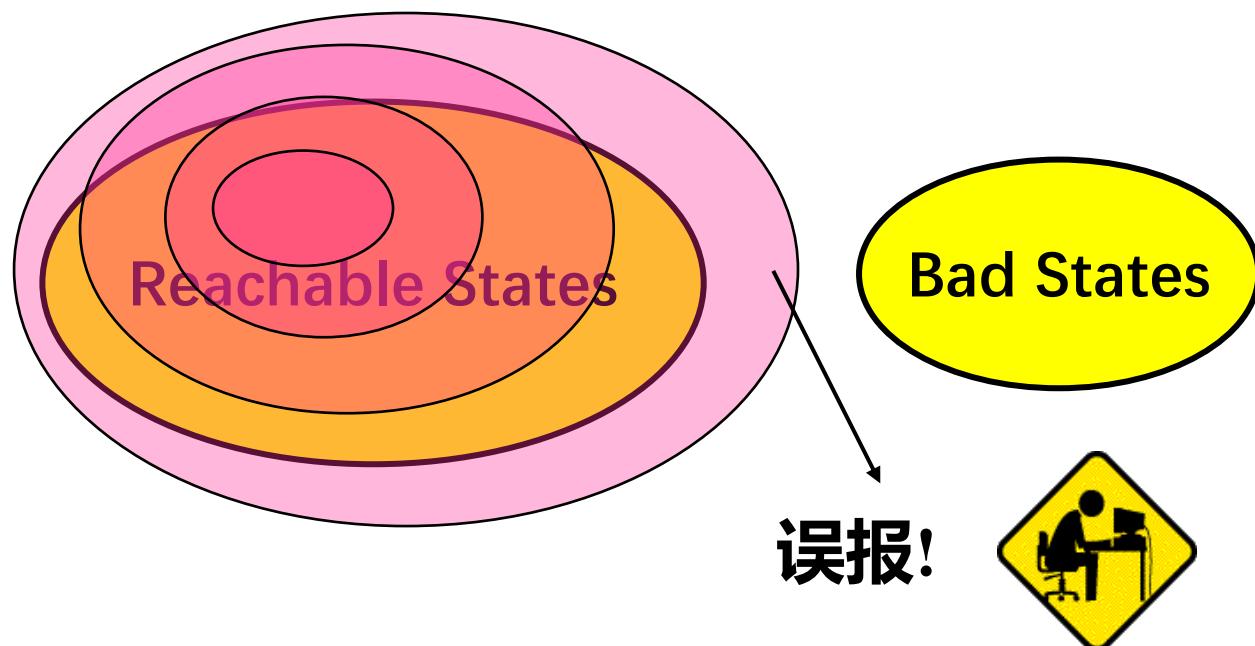
抽象元素特征

$$\pm x_i \leq c$$

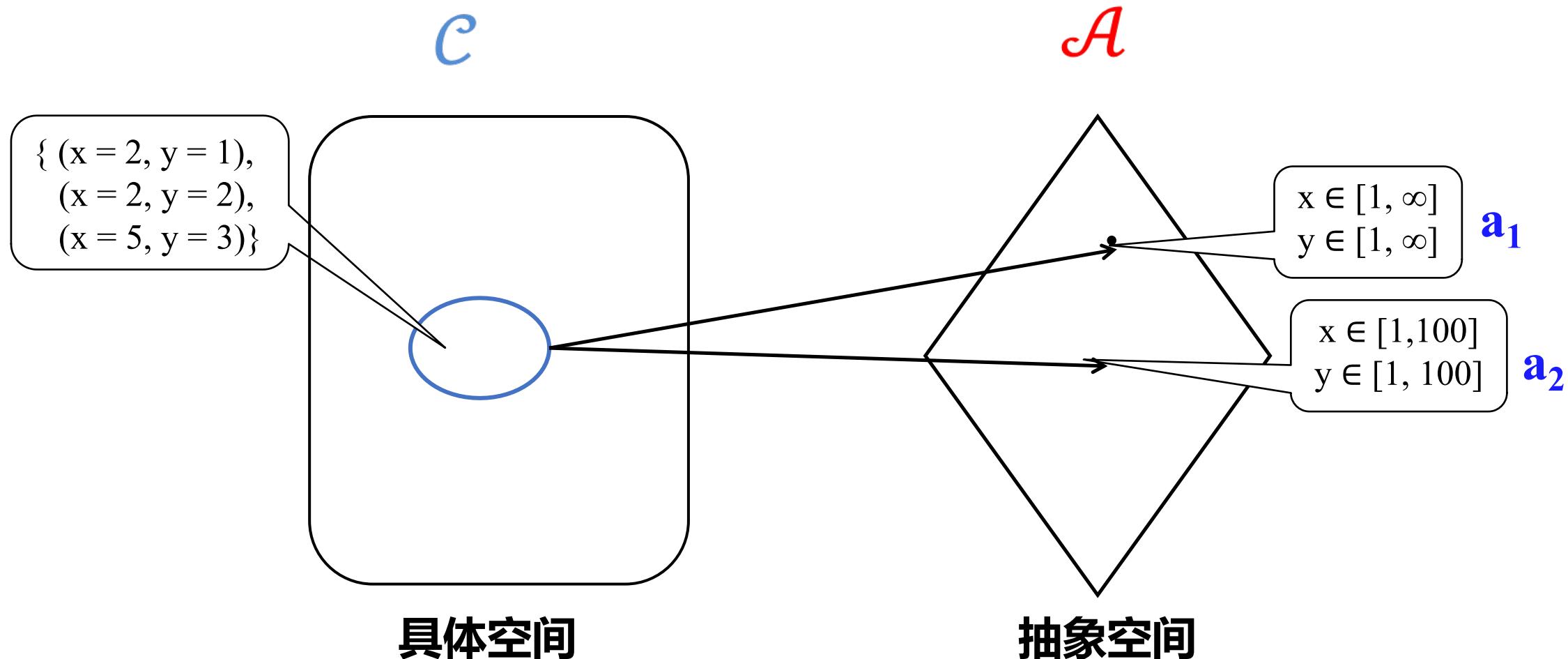
多面体域 [Cousot & Halbwach, POPL'78] $a_1 x_1 + a_2 x_2 + \dots + a_n x_n \leq c$

抽象解释的精度问题

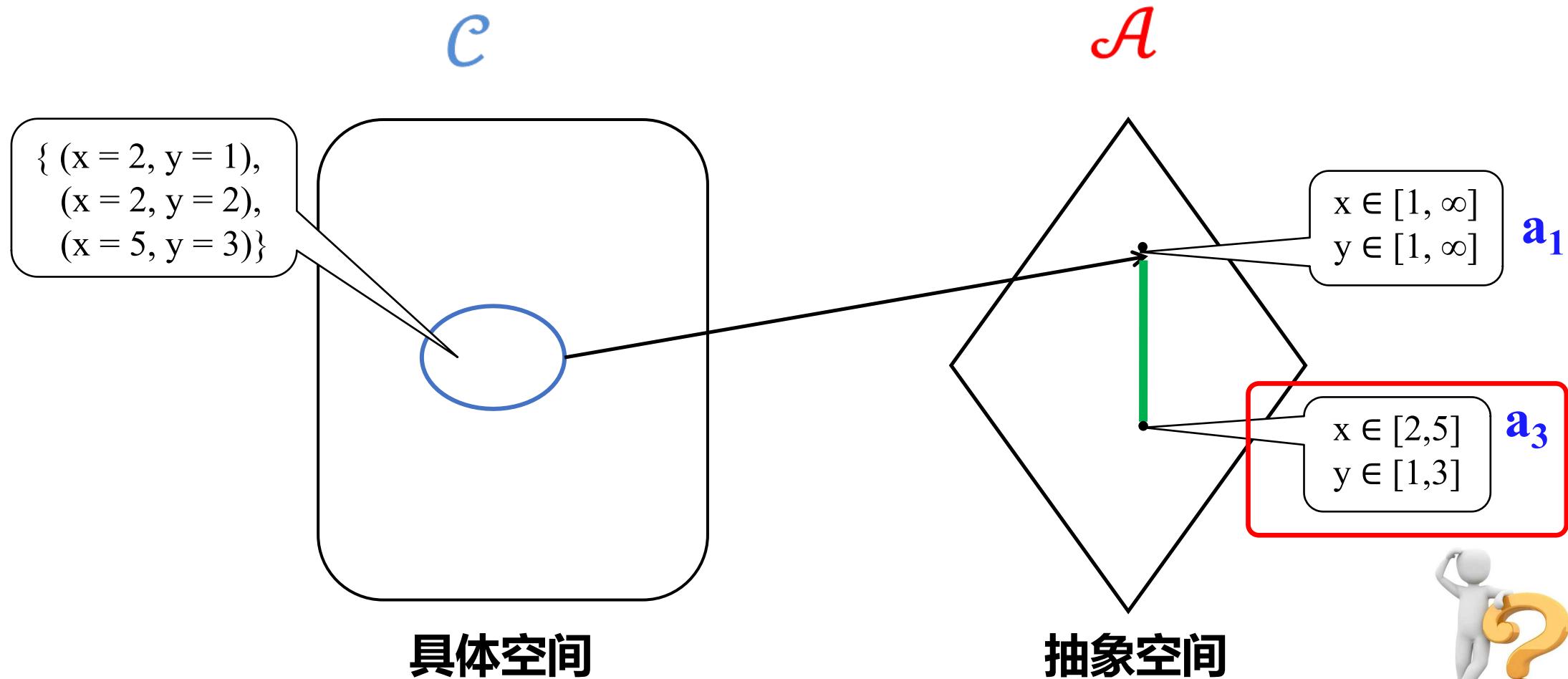
- 静态程序分析的核心理论 [Cousot & Cousot, POPL'77]
- 对程序的可达状态做上近似



例：区间域的精度问题



区间域下的最佳(最精确)抽象





最佳抽象的形式化定义

- 给定具体域 C 和抽象域 \mathcal{A} 之间的Galois连接

$$(C, \subseteq) \xrightleftharpoons[\alpha]{\gamma} (\mathcal{A}, \leq)$$

- 具体迁移函数 $F: C \rightarrow C$ 的最佳近似是 $F^\#$

$$F^\# \equiv \alpha \circ F \circ \gamma$$

问题: 以上 $F^\#$ 的定义是“非构造性”的



抽象解释理论

符号抽象框架

个人近期工作

一些相关问题



符号抽象：计算最佳抽象的框架

- *Symbolic implementation of the best transformer* [RSY, VMCAI'04]

输入: (1) 编码了程序具体语义的约束 φ ; (2) 抽象域 \mathcal{A} ,
输出: (2) 抽象领 \mathcal{A} 中能 *over-approximate* φ 的最小元素



Thomas
Reps



Mooly
Sagiv



Greta
Yorsh



符号抽象：逻辑意义上的刻画

- *Automating abstract interpretation* [Reps & Thakur, VMCAI'16]

\mathcal{L} 是表达力丰富的逻辑, 抽象域 \mathcal{A} 对应于 \mathcal{L} 的一个子集 \mathcal{L}' .
给定约束 $\varphi \in \mathcal{L}$, 找到它在 \mathcal{L}' 中的 **最强逻辑后承**



Thomas
Reps

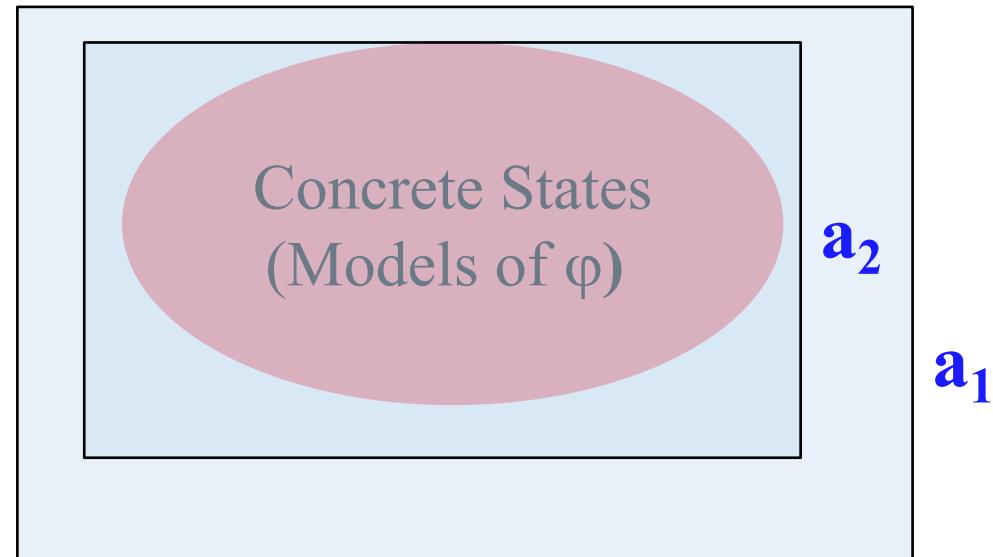


Aditya
Thakur

例: 符号抽象

- Automating abstract interpretation [Reps & Thakur, VMCAI'16]

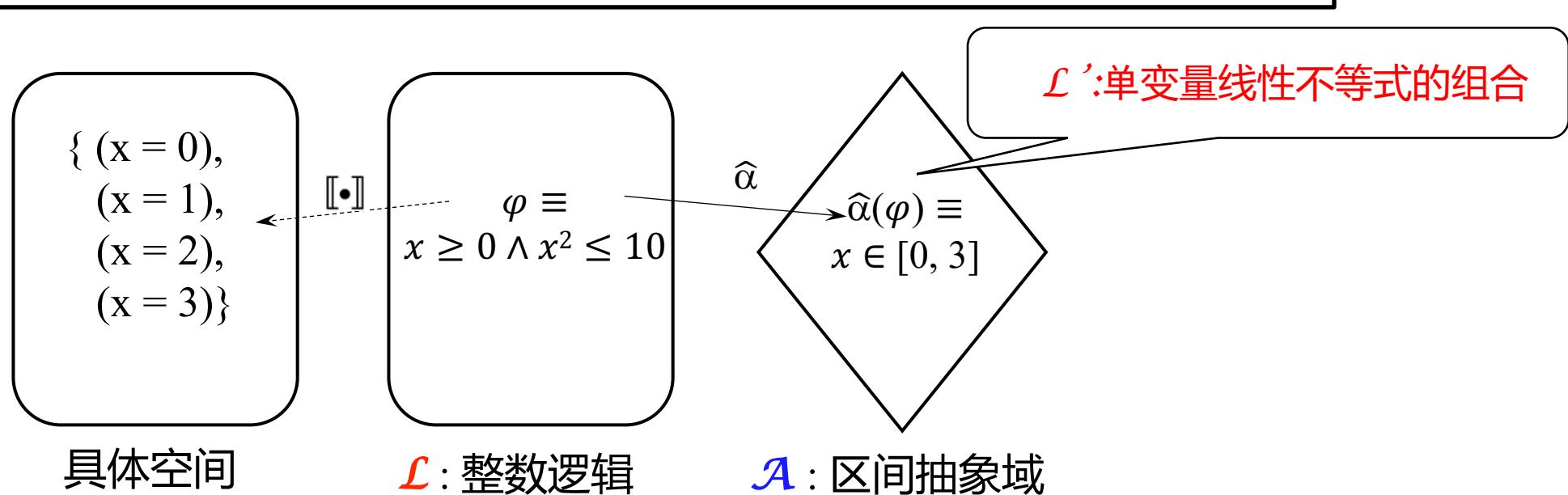
\mathcal{L} 是表达力丰富的逻辑, 抽象域 \mathcal{A} 对应于 \mathcal{L} 的一个子集 \mathcal{L}' :
给定约束 $\varphi \in \mathcal{L}$, 找到它在 \mathcal{L}' 中的 **最强逻辑后承**



例：符号抽象

- Automating abstract interpretation [Reps & Thakur, VMCAI'16]

\mathcal{L} 是表达力丰富的逻辑, 抽象域 \mathcal{A} 对应于 \mathcal{L} 的一个子集 \mathcal{L}' :
给定约束 $\varphi \in \mathcal{L}$, 找到它在 \mathcal{L}' 中的 **最强逻辑后承**





符号抽象的理论和实际意义

```
55
56 #include <algorithm>
57 #include <boost/bimap.hpp>
58 #include <boost/optional.hpp>
59
60     s_ldd_man = Ldd_Init(cudd, theory);
61     if (Params::dynamic_reordering) {
62         Cudd_AutodynEnable(cudd, CUDD_REORDER_GROUP_SIFT);
63     }
64     name[125] = "CUDD reorder threshold is quite arbitrary. A
65     unsigned threshold = num_of_vars() * Params::convexify_threshold;
66     /* 129 */ 563
67     /* T130 */ 565
68     /* 131 */ t566
69     /* 2 132 */ 567
70     /* 133 */ c568
71     /* F 134 */ 569
72     /* S 135 */ s570
73     /* S 136 */ 571
74     /* 137 */ i572
75     /* F 138 */ 573
76     /* 139 */ 574
77     /* temp 140 */ 575
78     /* 142 */ 576
79     /* clas 143 */ 577
80     /* 144 */ 578
81     /* 145 */ 579
82     /* us 146 */ 580
83     /* US 147 */ 581
84     /* US 148 */ 582
85     /* void forget(const variable_vector_t &variables) override { */
86     /* publ 150 */ 583
87     /* us 151 */ 584
88     /* us 152 */ 585
89     /* us 153 */ 586
90     /* us 154 */ 587
91     /* us 155 */ 588
92     /* us 156 */ 589
93     /* 157 */ i590
94     /* 158 */ 591
95     /* m 159 */ 592
96     /* 160 */ 593
97     /* 161 */ 594
98     /* 162 */ 595
99     /* enc 163 */ 596
100    /* 164 */ 597
101    /* 165 */ 598
102    /* 166 */ 599
103    /* 167 */ 600
104    /* 168 */ 601
105    /* 169 */ 602
106    /* 170 */ 603
107    /* 171 */ 604
108    /* 172 */ 605
109    /* 173 */ 606
110    /* 174 */ 607
111    /* 175 */ 608
112    /* 176 */ 609
113    /* 177 */ 610
114    /* 178 */ 611
115    /* 179 */ 612
116    /* 180 */ 613
117    /* 181 */ 614
118    /* 182 */ 615
119    /* 183 */ 616
120    /* 184 */ 617
121    /* 185 */ 618
122    /* 186 */ 619
123    /* 187 */ 620
124    /* 188 */ 621
125    /* 189 */ 622
126    /* 190 */ 623
127    /* 191 */ 624
128    /* 192 */ 625
129    /* 193 */ 626
130    /* 194 */ 627
131    /* 195 */ 628
132    /* 196 */ 629
133    /* 197 */ 630
134    /* 198 */ 631
135    /* 199 */ 632
136    /* 200 */ 633
137    /* 201 */ 634
138    /* 202 */ 635
139    /* 203 */ 636
140    /* 204 */ 637
141    /* 205 */ 638
142    /* 206 */ 639
143    /* 207 */ 640
144    /* 208 */ 641
145    /* 209 */ 642
146    /* 210 */ 643
147    /* 211 */ 644
148    /* 212 */ 645
149    /* 213 */ 646
150    /* 214 */ 647
151    /* 215 */ 648
152    /* 216 */ 649
153    /* 217 */ 650
154    /* 218 */ 651
155    /* 219 */ 652
156    /* 220 */ 653
157    /* 221 */ 654
158    /* 222 */ 655
159    /* 223 */ 656
160    /* 224 */ 657
161    /* 225 */ 658
162    /* 226 */ 659
163    /* 227 */ 660
164    /* 228 */ 661
165    /* 229 */ 662
166    /* 230 */ 663
167    /* 231 */ 664
168    /* 232 */ 665
169    /* 233 */ 666
170    /* 234 */ 667
171    /* 235 */ 668
172    /* 236 */ 669
173    /* 237 */ 670
174    /* 238 */ 671
175    /* 239 */ 672
176    /* 240 */ 673
177    /* 241 */ 674
178    /* 242 */ 675
179    /* 243 */ 676
180    /* 244 */ 677
181    /* 245 */ 678
182    /* 246 */ 679
183    /* 247 */ 680
184    /* 248 */ 681
185    /* 249 */ 682
186    /* 250 */ 683
187    /* 251 */ 684
188    /* 252 */ 685
189    /* 253 */ 686
190    /* 254 */ 687
191    /* 255 */ 688
192    /* 256 */ 689
193    /* 257 */ 690
194    /* 258 */ 691
195    /* 259 */ 692
196    /* 260 */ 693
197    /* 261 */ 694
198    /* 262 */ 695
199    /* 263 */ 696
200    /* 264 */ 697
201    /* 265 */ 698
202    /* 266 */ 699
203    /* 267 */ 700
204    /* 268 */ 701
205    /* 269 */ 702
206    /* 270 */ 703
207    /* 271 */ 704
208    /* 272 */ 705
209    /* 273 */ 706
210    /* 274 */ 707
211    /* 275 */ 708
212    /* 276 */ 709
213    /* 277 */ 710
214    /* 278 */ 711
215    /* 279 */ 712
216    /* 280 */ 713
217    /* 281 */ 714
218    /* 282 */ 715
219    /* 283 */ 716
220    /* 284 */ 717
221    /* 285 */ 718
222    /* 286 */ 719
223    /* 287 */ 720
224    /* 288 */ 721
225    /* 289 */ 722
226    /* 290 */ 723
227    /* 291 */ 724
228    /* 292 */ 725
229    /* 293 */ 726
230    /* 294 */ 727
231    /* 295 */ 728
232    /* 296 */ 729
233    /* 297 */ 730
234    /* 298 */ 731
235    /* 299 */ 732
236    /* 300 */ 733
237    /* 301 */ 734
238    /* 302 */ 735
239    /* 303 */ 736
240    /* 304 */ 737
241    /* 305 */ 738
242    /* 306 */ 739
243    /* 307 */ 740
244    /* 308 */ 741
245    /* 309 */ 742
246    /* 310 */ 743
247    /* 311 */ 744
248    /* 312 */ 745
249    /* 313 */ 746
250    /* 314 */ 747
251    /* 315 */ 748
252    /* 316 */ 749
253    /* 317 */ 750
254    /* 318 */ 751
255    /* 319 */ 752
256    /* 320 */ 753
257    /* 321 */ 754
258    /* 322 */ 755
259    /* 323 */ 756
260    /* 324 */ 757
261    /* 325 */ 758
262    /* 326 */ 759
263    /* 327 */ 760
264    /* 328 */ 761
265    /* 329 */ 762
266    /* 330 */ 763
267    /* 331 */ 764
268    /* 332 */ 765
269    /* 333 */ 766
270    /* 334 */ 767
271    /* 335 */ 768
272    /* 336 */ 769
273    /* 337 */ 770
274    /* 338 */ 771
275    /* 339 */ 772
276    /* 340 */ 773
277    /* 341 */ 774
278    /* 342 */ 775
279    /* 343 */ 776
280    /* 344 */ 777
281    /* 345 */ 778
282    /* 346 */ 779
283    /* 347 */ 780
284    /* 348 */ 781
285    /* 349 */ 782
286    /* 350 */ 783
287    /* 351 */ 784
288    /* 352 */ 785
289    /* 353 */ 786
290    /* 354 */ 787
291    /* 355 */ 788
292    /* 356 */ 789
293    /* 357 */ 790
294    /* 358 */ 791
295    /* 359 */ 792
296    /* 360 */ 793
297    /* 361 */ 794
298    /* 362 */ 795
299    /* 363 */ 796
300    /* 364 */ 797
301    /* 365 */ 798
302    /* 366 */ 799
303    /* 367 */ 800
304    /* 368 */ 801
305    /* 369 */ 802
306    /* 370 */ 803
307    /* 371 */ 804
308    /* 372 */ 805
309    /* 373 */ 806
310    /* 374 */ 807
311    /* 375 */ 808
312    /* 376 */ 809
313    /* 377 */ 810
314    /* 378 */ 811
315    /* 379 */ 812
316    /* 380 */ 813
317    /* 381 */ 814
318    /* 382 */ 815
319    /* 383 */ 816
320    /* 384 */ 817
321    /* 385 */ 818
322    /* 386 */ 819
323    /* 387 */ 820
324    /* 388 */ 821
325    /* 389 */ 822
326    /* 390 */ 823
327    /* 391 */ 824
328    /* 392 */ 825
329    /* 393 */ 826
330    /* 394 */ 827
331    /* 395 */ 828
332    /* 396 */ 829
333    /* 397 */ 830
334    /* 398 */ 831
335    /* 399 */ 832
336    /* 400 */ 833
337    /* 401 */ 834
338    /* 402 */ 835
339    /* 403 */ 836
340    /* 404 */ 837
341    /* 405 */ 838
342    /* 406 */ 839
343    /* 407 */ 840
344    /* 408 */ 841
345    /* 409 */ 842
346    /* 410 */ 843
347    /* 411 */ 844
348    /* 412 */ 845
349    /* 413 */ 846
350    /* 414 */ 847
351    /* 415 */ 848
352    /* 416 */ 849
353    /* 417 */ 850
354    /* 418 */ 851
355    /* 419 */ 852
356    /* 420 */ 853
357    /* 421 */ 854
358    /* 422 */ 855
359    /* 423 */ 856
360    /* 424 */ 857
361    /* 425 */ 858
362    /* 426 */ 859
363    /* 427 */ 860
364    /* 428 */ 861
365    /* 429 */ 862
366    /* 430 */ 863
367    /* 431 */ 864
368    /* 432 */ 865
369    /* 433 */ 866
370    /* 434 */ 867
371    /* 435 */ 868
372    /* 436 */ 869
373    /* 437 */ 870
374    /* 438 */ 871
375    /* 439 */ 872
376    /* 440 */ 873
377    /* 441 */ 874
378    /* 442 */ 875
379    /* 443 */ 876
380    /* 444 */ 877
381    /* 445 */ 878
382    /* 446 */ 879
383    /* 447 */ 880
384    /* 448 */ 881
385    /* 449 */ 882
386    /* 450 */ 883
387    /* 451 */ 884
388    /* 452 */ 885
389    /* 453 */ 886
390    /* 454 */ 887
391    /* 455 */ 888
392    /* 456 */ 889
393    /* 457 */ 890
394    /* 458 */ 891
395    /* 459 */ 892
396    /* 460 */ 893
397    /* 461 */ 894
398    /* 462 */ 895
399    /* 463 */ 896
360    /* 464 */ 897
361    /* 465 */ 898
362    /* 466 */ 899
363    /* 467 */ 900
364    /* 468 */ 901
365    /* 469 */ 902
366    /* 470 */ 903
367    /* 471 */ 904
368    /* 472 */ 905
369    /* 473 */ 906
370    /* 474 */ 907
371    /* 475 */ 908
372    /* 476 */ 909
373    /* 477 */ 910
374    /* 478 */ 911
375    /* 479 */ 912
376    /* 480 */ 913
377    /* 481 */ 914
378    /* 482 */ 915
379    /* 483 */ 916
380    /* 484 */ 917
381    /* 485 */ 918
382    /* 486 */ 919
383    /* 487 */ 920
384    /* 488 */ 921
385    /* 489 */ 922
386    /* 490 */ 923
387    /* 491 */ 924
388    /* 492 */ 925
389    /* 493 */ 926
390    /* 494 */ 927
391    /* 495 */ 928
392    /* 496 */ 929
393    /* 497 */ 930
394    /* 498 */ 931
395    /* 499 */ 932
396    /* 500 */ 933
397    /* 501 */ 934
398    /* 502 */ 935
399    /* 503 */ 936
360    /* 504 */ 937
361    /* 505 */ 938
362    /* 506 */ 939
363    /* 507 */ 940
364    /* 508 */ 941
365    /* 509 */ 942
366    /* 510 */ 943
367    /* 511 */ 944
368    /* 512 */ 945
369    /* 513 */ 946
370    /* 514 */ 947
371    /* 515 */ 948
372    /* 516 */ 949
373    /* 517 */ 950
374    /* 518 */ 951
375    /* 519 */ 952
376    /* 520 */ 953
377    /* 521 */ 954
378    /* 522 */ 955
379    /* 523 */ 956
380    /* 524 */ 957
381    /* 525 */ 958
382    /* 526 */ 959
383    /* 527 */ 960
384    /* 528 */ 961
385    /* 529 */ 962
386    /* 530 */ 963
387    /* 531 */ 964
388    /* 532 */ 965
389    /* 533 */ 966
390    /* 534 */ 967
391    /* 535 */ 968
392    /* 536 */ 969
393    /* 537 */ 970
394    /* 538 */ 971
395    /* 539 */ 972
396    /* 540 */ 973
397    /* 541 */ 974
398    /* 542 */ 975
399    /* 543 */ 976
360    /* 544 */ 977
361    /* 545 */ 978
362    /* 546 */ 979
363    /* 547 */ 980
364    /* 548 */ 981
365    /* 549 */ 982
366    /* 550 */ 983
367    /* 551 */ 984
368    /* 552 */ 985
369    /* 553 */ 986
370    /* 554 */ 987
371    /* 555 */ 988
372    /* 556 */ 989
373    /* 557 */ 990
374    /* 558 */ 991
375    /* 559 */ 992
376    /* 560 */ 993
377    /* 561 */ 994
378    /* 562 */ 995
379    /* 563 */ 996
380    /* 564 */ 997
381    /* 565 */ 998
382    /* 566 */ 999
383    /* 567 */ 1000
384    /* 568 */ 1001
385    /* 569 */ 1002
386    /* 570 */ 1003
387    /* 571 */ 1004
388    /* 572 */ 1005
389    /* 573 */ 1006
390    /* 574 */ 1007
391    /* 575 */ 1008
392    /* 576 */ 1009
393    /* 577 */ 1010
394    /* 578 */ 1011
395    /* 579 */ 1012
396    /* 580 */ 1013
397    /* 581 */ 1014
398    /* 582 */ 1015
399    /* 583 */ 1016
360    /* 584 */ 1017
361    /* 585 */ 1018
362    /* 586 */ 1019
363    /* 587 */ 1020
364    /* 588 */ 1021
365    /* 589 */ 1022
366    /* 590 */ 1023
367    /* 591 */ 1024
368    /* 592 */ 1025
369    /* 593 */ 1026
370    /* 594 */ 1027
371    /* 595 */ 1028
372    /* 596 */ 1029
373    /* 597 */ 1030
374    /* 598 */ 1031
375    /* 599 */ 1032
376    /* 600 */ 1033
377    /* 601 */ 1034
378    /* 602 */ 1035
379    /* 603 */ 1036
380    /* 604 */ 1037
381    /* 605 */ 1038
382    /* 606 */ 1039
383    /* 607 */ 1040
384    /* 608 */ 1041
385    /* 609 */ 1042
386    /* 610 */ 1043
387    /* 611 */ 1044
388    /* 612 */ 1045
389    /* 613 */ 1046
390    /* 614 */ 1047
391    /* 615 */ 1048
392    /* 616 */ 1049
393    /* 617 */ 1050
394    /* 618 */ 1051
395    /* 619 */ 1052
396    /* 620 */ 1053
397    /* 621 */ 1054
398    /* 622 */ 1055
399    /* 623 */ 1056
360    /* 624 */ 1057
361    /* 625 */ 1058
362    /* 626 */ 1059
363    /* 627 */ 1060
364    /* 628 */ 1061
365    /* 629 */ 1062
366    /* 630 */ 1063
367    /* 631 */ 1064
368    /* 632 */ 1065
369    /* 633 */ 1066
370    /* 634 */ 1067
371    /* 635 */ 1068
372    /* 636 */ 1069
373    /* 637 */ 1070
374    /* 638 */ 1071
375    /* 639 */ 1072
376    /* 640 */ 1073
377    /* 641 */ 1074
378    /* 642 */ 1075
379    /* 643 */ 1076
380    /* 644 */ 1077
381    /* 645 */ 1078
382    /* 646 */ 1079
383    /* 647 */ 1080
384    /* 648 */ 1081
385    /* 649 */ 1082
386    /* 650 */ 1083
387    /* 651 */ 1084
388    /* 652 */ 1085
389    /* 653 */ 1086
390    /* 654 */ 1087
391    /* 655 */ 1088
392    /* 656 */ 1089
393    /* 657 */ 1090
394    /* 658 */ 1091
395    /* 659 */ 1092
396    /* 660 */ 1093
397    /* 661 */ 1094
398    /* 662 */ 1095
399    /* 663 */ 1096
360    /* 664 */ 1097
361    /* 665 */ 1098
362    /* 666 */ 1099
363    /* 667 */ 1100
364    /* 668 */ 1101
365    /* 669 */ 1102
366    /* 670 */ 1103
367    /* 671 */ 1104
368    /* 672 */ 1105
369    /* 673 */ 1106
370    /* 674 */ 1107
371    /* 675 */ 1108
372    /* 676 */ 1109
373    /* 677 */ 1110
374    /* 678 */ 1111
375    /* 679 */ 1112
376    /* 680 */ 1113
377    /* 681 */ 1114
378    /* 682 */ 1115
379    /* 683 */ 1116
380    /* 684 */ 1117
381    /* 685 */ 1118
382    /* 686 */ 1119
383    /* 687 */ 1120
384    /* 688 */ 1121
385    /* 689 */ 1122
386    /* 690 */ 1123
387    /* 691 */ 1124
388    /* 692 */ 1125
389    /* 693 */ 1126
390    /* 694 */ 1127
391    /* 695 */ 1128
392    /* 696 */ 1129
393    /* 697 */ 1130
394    /* 698 */ 1131
395    /* 699 */ 1132
396    /* 700 */ 1133
397    /* 701 */ 1134
398    /* 702 */ 1135
399    /* 703 */ 1136
360    /* 704 */ 1137
361    /* 705 */ 1138
362    /* 706 */ 1139
363    /* 707 */ 1140
364    /* 708 */ 1141
365    /* 709 */ 1142
366    /* 710 */ 1143
367    /* 711 */ 1144
368    /* 712 */ 1145
369    /* 713 */ 1146
370    /* 714 */ 1147
371    /* 715 */ 1148
372    /* 716 */ 1149
373    /* 717 */ 1150
374    /* 718 */ 1151
375    /* 719 */ 1152
376    /* 720 */ 1153
377    /* 721 */ 1154
378    /* 722 */ 1155
379    /* 723 */ 1156
380    /* 724 */ 1157
381    /* 725 */ 1158
382    /* 726 */ 1159
383    /* 727 */ 1160
384    /* 728 */ 1161
385    /* 729 */ 1162
386    /* 730 */ 1163
387    /* 731 */ 1164
388    /* 732 */ 1165
389    /* 733 */ 1166
390    /* 734 */ 1167
391    /* 735 */ 1168
392    /* 736 */ 1169
393    /* 737 */ 1170
394    /* 738 */ 1171
395    /* 739 */ 1172
396    /* 740 */ 1173
397    /* 741 */ 1174
398    /* 742 */ 1175
399    /* 743 */ 1176
360    /* 744 */ 1177
361    /* 745 */ 1178
362    /* 746 */ 1179
363    /* 747 */ 1180
364    /* 748 */ 1181
365    /* 749 */ 1182
366    /* 750 */ 1183
367    /* 751 */ 1184
368    /* 752 */ 1185
369    /* 753 */ 1186
370    /* 754 */ 1187
371    /* 755 */ 1188
372    /* 756 */ 1189
373    /* 757 */ 1190
374    /* 758 */ 1191
375    /* 759 */ 1192
376    /* 760 */ 1193
377    /* 761 */ 1194
378    /* 762 */ 1195
379    /* 763 */ 1196
380    /* 764 */ 1197
381    /* 765 */ 1198
382    /* 766 */ 1199
383    /* 767 */ 1200
384    /* 768 */ 1201
385    /* 769 */ 1202
386    /* 770 */ 1203
387    /* 771 */ 1204
388    /* 772 */ 1205
389    /* 773 */ 1206
390    /* 774 */ 1207
391    /* 775 */ 1208
392    /* 776 */ 1209
393    /* 777 */ 1210
394    /* 778 */ 1211
395    /* 779 */ 1212
396    /* 780 */ 1213
397    /* 781 */ 1214
398    /* 782 */ 1215
399    /* 783 */ 1216
360    /* 784 */ 1217
361    /* 785 */ 1218
362    /* 786 */ 1219
363    /* 787 */ 1220
364    /* 788 */ 1221
365    /* 789 */ 1222
366    /* 790 */ 1223
367    /* 791 */ 1224
368    /* 792 */ 1225
369    /* 793 */ 1226
370    /* 794 */ 1227
371    /* 795 */ 1228
372    /* 796 */ 1229
373    /* 797 */ 1230
374    /* 798 */ 1231
375    /* 799 */ 1232
376    /* 800 */ 1233
377    /* 801 */ 1234
378    /* 802 */ 1235
379    /* 803 */ 1236
380    /* 804 */ 1237
381    /* 805 */ 1238
382    /* 806 */ 1239
383    /* 807 */ 1240
384    /* 808 */ 1241
385    /* 809 */ 1242
386    /* 810 */ 1243
387    /* 811 */ 1244
388    /* 812 */ 1245
389    /* 813 */ 1246
390    /* 814 */ 1247
391    /* 815 */ 1248
392    /* 816 */ 1249
393    /* 817 */ 1250
394    /* 818 */ 1251
395    /* 819 */ 1252
396    /* 820 */ 1253
397    /* 821 */ 1254
398    /* 822 */ 1255
399    /* 823 */ 1256
360    /* 824 */ 1257
361    /* 825 */ 1258
362    /* 826 */ 1259
363    /* 827 */ 1260
364    /* 828 */ 1261
365    /* 829 */ 1262
366    /* 830 */ 1263
367    /* 831 */ 1264
368    /* 832 */ 1265
369    /* 833 */ 1266
370    /* 834 */ 1267
371    /* 835 */ 1268
372    /* 836 */
```



符号抽象的(少量)应用

- 源代码分析
 - 形态分析 [RSY, VMCAI'04; Yorsh et al., SAS'04]
 - 数值验证 [Li et al., POPL'14; Jiang el al., VMCAI'17]
- 二进制分析
 - 区间和集合域 [Barrett et al., ENTCS'10; Brauer et al., ESOP'11]
 - 线性等式域 [King et al., VMCAI'10; Thakur et al., SAS'12; Elder et al., TOPLAS'14]

应用于**工业级**二进制分析产品
 **GRAMMATECH**

在形式化/编程语言、甚至抽象解释社区都还不够普及



报告提纲

抽象解释理论

符号抽象框架

个人近期工作 (这部分略过)

一些相关问题



报告提纲

抽象解释理论

符号抽象框架

个人近期工作

一些相关问题



符号抽象相关问题

\mathcal{L} 是表达力丰富的逻辑, 抽象域 \mathcal{A} 对应于 \mathcal{L} 的一个子集 \mathcal{L}' :
给定 $\varphi \in \mathcal{L}$, 找到它在 \mathcal{L}' 中的最强逻辑后承

- **形式化方法: 谓词抽象** [Graf & Saidi 97]
 - $\varphi \in \mathcal{L}$: 编码了一个(不带循环的)程序块的约束
 - \mathcal{L}' : 给定谓词集合 $\{P_1, \dots, P_n\}$ 的任意布尔组合



Software Model Checking领域的“开山之作”



符号抽象相关问题

\mathcal{L} 是表达力丰富的逻辑, 抽象域 \mathcal{A} 对应于 \mathcal{L} 的一个子集 \mathcal{L}' :
给定 $\varphi \in \mathcal{L}$, 找到它在 \mathcal{L}' 中的 **最强逻辑后承**

- **形式化方法**
 - 谓词抽象 [Graf & Saidi 97] \mathcal{L}' : 给定谓词集合 $\{P_1, \dots, P_n\}$ 的布尔组合
- **自动推理: 量词消去**
 - $\varphi \in \mathcal{L}$: 任意形式的整数/实数/浮点/字符/...约束
 - \mathcal{L}' : 只使用给定约束变量集合 $S \subseteq Vars(\varphi)$ 的约束

Z3

 WOLFRAM
MATHEMATICA 11



符号抽象相关问题

\mathcal{L} 是表达力丰富的逻辑, 抽象域 \mathcal{A} 对应于 \mathcal{L} 的一个子集 \mathcal{L}' :
给定 $\varphi \in \mathcal{L}$, 找到它在 \mathcal{L}' 中的最强逻辑后承

- **形式化方法**
 - 谓词抽象 [Graf & Saidi 97] \mathcal{L}' : 给定谓词集合 $\{P_1, \dots, P_n\}$ 的布尔组合
- **自动推理**
 - 量词消去 \mathcal{L}' : 使用给定约束变量集合 $S \subseteq Vars(\varphi)$ 的约束
- **人工智能**
 - Forgetting [Lin & Reita 94] \mathcal{L}' : 类似量词消去问题



符号抽象相关问题

\mathcal{L} 是表达力丰富的逻辑, 抽象域 \mathcal{A} 对应于 \mathcal{L} 的一个子集 \mathcal{L}' :
给定 $\varphi \in \mathcal{L}$, 找到它在 \mathcal{L}' 中的最强逻辑后承

- **形式化方法**
 - 谓词抽象 [Graf & Saidi 97] \mathcal{L}' : 给定谓词集合 $\{P_1, \dots, P_n\}$ 的布尔组合
- **自动推理**
 - 量词消去 \mathcal{L}' : 使用给定约束变量集合 $S \subseteq Vars(\varphi)$ 的约束
- **人工智能**
 - Forgetting [Lin & Reita 94] \mathcal{L}' : 类似量词消去问题
- **运筹学**
 - 线性规划 \mathcal{L} 线性约束集合; \mathcal{L}' : $f(X) \leq c$ (f 是线性目标函数)



总结与展望: 程序合成视角

Automating abstract interpretation [Reps & Thakur, VMCAI'16]

程序合成: 如何自动从规约中生成程序



“One of the most central problems in the theory of programming.”

----Amir Pneuli

1996年图灵奖获得者

“(软件自动化)提升软件生产率的根本途径”

----徐家福先生

中国软件先驱



感谢聆听！

pyaoaa@zju.edu.cn