

# BOOLEAN PROGRAM EXPLORATION USING AN ALL-SAT SOLVER BACKEND

Peizun Liu and Thomas Wahl, Northeastern University, Boston, USA

SAT/SMT Summer School, Semmering, Austria, July 10-12, 2014



## PROBLEM

**Program state reachability analysis** for replicated Boolean programs run by an unbounded number of threads is decidable in principle via a reduction of the Boolean program families to *well-structured transition systems* (WSTS). The obtained transition systems would, however, in general be intractably large, due to local state explosion:

<#A000: 3, #A001: 0, #A002: 0, #A003: 0, #A004: 0, #A005: 0, #A006: 0, #A007: 0, #A008: 0, #A009: 0, #A010: 0, #A011: 0, #A012: 0, #A013: 0, #A014: 0, #A015: 0, #A016: 0, #A017: 0, #A018: 0, #A019: 0, #A020: 0, #A021: 0, #A022: 0, #A023: 0, #A024: 0, #A025: 0, #A026: 0, #A027: 0, #A028: 0, #A029: 0, #A030: 0, #A031: 0, #A032: 0, #A033: 0, #A034: 0, #A035: 0, #A036: 0, #A037: 0, #A038: 0, #A039: 0, #A040: 0, #A041: 0, #A042: 0, #A043: 0, #A044: 0, #A045: 0, #A046: 0, #A047: 0, #A048: 0, #A049: 0, #A050: 0, #A051: 0, #A052: 0, #A053: 0, #A054: 0, #A055: 0, #A056: 0, #A057: 0, #A058: 0, #A059: 0, #A060: 0, #A061: 0, #A062: 0, #A063: 0, #A064: 0, #A065: 0, #A066: 0, #A067: 0, #A068: 0, #A069: 0, #A070: 0, #A071: 0, #A072: 0, #A073: 0, #A074: 0, #A075: 0, #A076: 0, #A077: 0, #A078: 0, #A079: 0, #A080: 0, #A081: 0, #A082: 0, #A083: 0, #A084: 0, #A085: 0, #A086: 0, #A087: 0, #A088: 0, #A089: 0, #A090: 0, #A091: 0, #A092: 0, #A093: 0, #A094: 0, #A095: 0, #A096: 0, #A097: 0, #A098: 0, #A099: 0, #A100: 0, #A101: 0, #A102: 0, #A103: 0, #A104: 0, #A105: 0, #A106: 0, #A107: 0, #A108: 0, #A109: 0, #A110: 0, #A111: 0, #A112: 0, #A113: 0, #A114: 0, #A115: 0, #A116: 0, #A117: 0, #A118: 0, #A119: 0, #A120: 0, #A121: 0, #A122: 0, #A123: 0, #A124: 0, #A125: 0, #A126: 0, #A127: 0, #A128: 0, #A129: 0, #A130: 0, #A131: 0, #A132: 0, #A133: 0, #A134: 0, #A135: 0, #A136: 0, #A137: 0, #A138: 0, #A139: 0, #A140: 0, #A141: 0, #A142: 0, #A143: 0, #A144: 0, #A145: 0, #A146: 0, #A147: 0, #A148: 0, #A149: 0, #A150: 0, #A151: 0, #A152: 0, #A153: 0, #A154: 0, #A155: 0, #A156: 0, #A157: 0, #A158: 0, #A159: 0, #A160: 0, #A161: 0, #A162: 0, #A163: 0, #A164: 0, #A165: 0, #A166: 0, #A167: 0, #A168: 0, #A169: 0, #A170: 0, #A171: 0, #A172: 0, #A173: 0, #A174: 0, #A175: 0, #A176: 0, #A177: 0, #A178: 0, #A179: 0, #A180: 0, #A181: 0, #A182: 0, #A183: 0, #A184: 0, #A185: 0, #A186: 0, #A187: 0, #A188: 0, #A189: 0, #A190: 0, #A191: 0, #A192: 0, #A193: 0, #A194: 0, #A195: 0, #A196: 0, #A197: 0, #A198: 0, #A199: 0, #A200: 0, #A201: 0, #A202: 0, #A203: 0, #A204: 0, #A205: 0, #A206: 0, #A207: 0, #A208: 0, #A209: 0, #A210: 0, #A211: 0, #A212: 0, #A213: 0, #A214: 0, #A215: 0, #A216: 0, #A217: 0, #A218: 0, #A219: 0, #A220: 0, #A221: 0, #A222: 0, #A223: 0, #A224: 0, #A225: 0, #A226: 0, #A227: 0, #A228: 0, #A229: 0, #A230: 0, #A231: 0, #A232: 0, #A233: 0, #A234: 0, #A235: 0, #A236: 0, #A237: 0, #A238: 0, #A239: 0, #A240: 0, #A241: 0, #A242: 0, #A243: 0, #A244: 0, #A245: 0, #A246: 0, #A247: 0, #A248: 0, #A249: 0, #A250: 0, #A251: 0, #A252: 0, #A253: 0, #A254: 0, #A255: 0, #A256: 0, #A257: 0, #A258: 0, #A259: 0, #A260: 0, #A261: 0, #A262: 0, #A263: 0, #A264: 0, #A265: 0, #A266: 0, #A267: 0, #A268: 0, #A269: 0, #A270: 0, #A271: 0, #A272: 0, #A273: 0, #A274: 0, #A275: 0, #A276: 0, #A277: 0, #A278: 0, #A279: 0, #A280: 0, #A281: 0, #A282: 0, #A283: 0, #A284: 0, #A285: 0, #A286: 0, #A287: 0, #A288: 0, #A289: 0, #A290: 0, #A291: 0, #A292: 0, #A293: 0, #A294: 0, #A295: 0, #A296: 0, #A297: 0, #A298: 0, #A299: 0, #A300: 0, #A301: 0, #A302: 0, #A303: 0, #A304: 0, #A305: 0, #A306: 0, #A307: 0, #A308: 0, #A309: 0, #A310: 0, #A311: 0, #A312: 0, #A313: 0, #A314: 0, #A315: 0, #A316: 0, #A317: 0, #A318: 0, #A319: 0, #A320: 0, #A321: 0, #A322: 0, #A323: 0, #A324: 0, #A325: 0, #A326: 0, #A327: 0, #A328: 0, #A329: 0, #A330: 0, #A331: 0, #A332: 0, #A333: 0, #A334: 0, #A335: 0, #A336: 0, #A337: 0, #A338: 0, #A339: 0, #A340: 0, #A341: 0, #A342: 0, #A343: 0, #A344: 0, #A345: 0, #A346: 0, #A347: 0, #A348: 0, #A349: 0, #A350: 0, #A351: 0, #A352: 0, #A353: 0, #A354: 0, #A355: 0, #A356: 0, #A357: 0, #A358: 0, #A359: 0, #A360: 0, #A361: 0, #A362: 0, #A363: 0, #A364: 0, #A365: 0, #A366: 0, #A367: 0, #A368: 0, #A369: 0, #A370: 0, #A371: 0, #A372: 0, #A373: 0, #A374: 0, #A375: 0, #A376: 0, #A377: 0, #A378: 0, #A379: 0, #A380: 0, #A381: 0, #A382: 0, #A383: 0, #A384: 0, #A385: 0, #A386: 0, #A387: 0, #A388: 0, #A389: 0, #A390: 0, #A391: 0, #A392: 0, #A393: 0, #A394: 0, #A395: 0, #A396: 0, #A397: 0, #A398: 0, #A399: 0, #A400: 0, #A401: 0, #A402: 0, #A403: 0, #A404: 0, #A405: 0, #A406: 0, #A407: 0, #A408: 0, #A409: 0, #A410: 0, #A411: 0, #A412: 0, #A413: 0, #A414: 0, #A415: 0, #A416: 0, #A417: 0, #A418: 0, #A419: 0, #A420: 0, #A421: 0, #A422: 0, #A423: 0, #A424: 0, #A425: 0, #A426: 0, #A427: 0, #A428: 0, #A429: 0, #A430: 0, #A431: 0, #A432: 0, #A433: 0, #A434: 0, #A435: 0, #A436: 0, #A437: 0, #A438: 0, #A439: 0, #A440: 0, #A441: 0, #A442: 0, #A443: 0, #A444: 0, #A445: 0, #A446: 0, #A447: 0, #A448: 0, #A449: 0, #A450: 0, #A451: 0, #A452: 0, #A453: 0, #A454: 0, #A455: 0, #A456: 0, #A457: 0, #A458: 0, #A459: 0, #A460: 0, #A461: 0, #A462: 0, #A463: 0, #A464: 0, #A465: 0, #A466: 0, #A467: 0, #A468: 0, #A469: 0, #A470: 0, #A471: 0, #A472: 0, #A473: 0, #A474: 0, #A475: 0, #A476: 0, #A477: 0, #A478: 0, #A479: 0, #A480: 0, #A481: 0, #A482: 0, #A483: 0, #A484: 0, #A485: 0, #A486: 0, #A487: 0, #A488: 0, #A489: 0, #A490: 0, #A491: 0, #A492: 0, #A493: 0, #A494: 0, #A495: 0, #A496: 0, #A497: 0, #A498: 0, #A499: 0, #A500: 0, #A501: 0, #A502: 0, #A503: 0, #A504: 0, #A505: 0, #A506: 0, #A507: 0, #A508: 0, #A509: 0, #A510: 0, #A511: 0, #A512: 0, #A513: 0, #A514: 0, #A515: 0, #A516: 0, #A517: 0, #A518: 0, #A519: 0, #A520: 0, #A521: 0, #A522: 0, #A523: 0, #A524: 0, #A525: 0, #A526: 0, #A527: 0, #A528: 0, #A529: 0, #A530: 0, #A531: 0, #A532: 0, #A533: 0, #A534: 0, #A535: 0, #A536: 0, #A537: 0, #A538: 0, #A539: 0, #A540: 0, #A541: 0, #A542: 0, #A543: 0, #A544: 0, #A545: 0, #A546: 0, #A547: 0, #A548: 0, #A549: 0, #A550: 0, #A551: 0, #A552: 0, #A553: 0, #A554: 0, #A555: 0, #A556: 0, #A557: 0, #A558: 0, #A559: 0, #A560: 0, #A561: 0, #A562: 0, #A563: 0, #A564: 0, #A565: 0, #A566: 0, #A567: 0, #A568: 0, #A569: 0, #A570: 0, #A571: 0, #A572: 0, #A573: 0, #A574: 0, #A575: 0, #A576: 0, #A577: 0, #A578: 0, #A579: 0, #A580: 0, #A581: 0, #A582: 0, #A583: 0, #A584: 0, #A585: 0, #A586: 0, #A587: 0, #A588: 0, #A589: 0, #A590: 0, #A591: 0, #A592: 0, #A593: 0, #A594: 0, #A595: 0, #A596: 0, #A597: 0, #A598: 0, #A599: 0, #A600: 0, #A601: 0, #A602: 0, #A603: 0, #A604: 0, #A605: 0, #A606: 0, #A607: 0, #A608: 0, #A609: 0, #A610: 0, #A611: 0, #A612: 0, #A613: 0, #A614: 0, #A615: 0, #A616: 0, #A617: 0, #A618: 0, #A619: 0, #A620: 0, #A621: 0, #A622: 0, #A623: 0, #A624: 0, #A625: 0, #A626: 0, #A627: 0, #A628: 0, #A629: 0, #A630: 0, #A631: 0, #A632: 0, #A633: 0, #A634: 0, #A635: 0, #A636: 0, #A637: 0, #A638: 0, #A639: 0, #A640: 0, #A641: 0, #A642: 0, #A643: 0, #A644: 0, #A645: 0, #A646: 0, #A647: 0, #A648: 0, #A649: 0, #A650: 0, #A651: 0, #A652: 0, #A653: 0, #A654: 0, #A655: 0, #A656: 0, #A657: 0, #A658: 0, #A659: 0, #A660: 0, #A661: 0, #A662: 0, #A663: 0, #A664: 0, #A665: 0, #A666: 0, #A667: 0, #A668: 0, #A669: 0, #A670: 0, #A671: 0, #A672: 0, #A673: 0, #A674: 0, #A675: 0, #A676: 0, #A677: 0, #A678: 0, #A679: 0, #A680: 0, #A681: 0, #A682: 0, #A683: 0, #A684: 0, #A685: 0, #A686: 0, #A687: 0, #A688: 0, #A689: 0, #A690: 0, #A691: 0, #A692: 0, #A693: 0, #A694: 0, #A695: 0, #A696: 0, #A697: 0, #A698: 0, #A699: 0, #A700: 0, #A701: 0, #A702: 0, #A703: 0, #A704: 0, #A705: 0, #A706: 0, #A707: 0, #A708: 0, #A709: 0, #A710: 0, #A711: 0, #A712: 0, #A713: 0, #A714: 0, #A715: 0, #A716: 0, #A717: 0, #A718: 0, #A719: 0, #A720: 0, #A721: 0, #A722: 0, #A723: 0, #A724: 0, #A725: 0, #A726: 0, #A727: 0, #A728: 0, #A729: 0, #A730: 0, #A731: 0, #A732: 0, #A733: 0, #A734: 0, #A735: 0, #A736: 0, #A737: 0, #A738: 0, #A739: 0, #A740: 0, #A741: 0, #A742: 0, #A743: 0, #A744: 0, #A745: 0, #A746: 0, #A747: 0, #A748: 0, #A749: 0, #A750: 0, #A751: 0, #A752: 0, #A753: 0, #A754: 0, #A755: 0, #A756: 0, #A757: 0, #A758: 0, #A759: 0, #A760: 0, #A761: 0, #A762: 0, #A763: 0, #A764: 0, #A765: 0, #A766: 0, #A767: 0, #A768: 0, #A769: 0, #A770: 0, #A771: 0, #A772: 0, #A773: 0, #A774: 0, #A775: 0, #A776: 0, #A777: 0, #A778: 0, #A779: 0, #A780: 0, #A781: 0, #A782: 0, #A783: 0, #A784: 0, #A785: 0, #A786: 0, #A787: 0, #A788: 0, #A789: 0, #A790: 0, #A791: 0, #A792: 0, #A793: 0, #A794: 0, #A795: 0, #A796: 0, #A797: 0, #A798: 0, #A799: 0, #A800: 0, #A801: 0, #A802: 0, #A803: 0, #A804: 0, #A805: 0, #A806: 0, #A807: 0, #A808: 0, #A809: 0, #A810: 0, #A811: 0, #A812: 0, #A813: 0, #A814: 0, #A815: 0, #A816: 0, #A817: 0, #A818: 0, #A819: 0, #A820: 0, #A821: 0, #A822: 0, #A823: 0, #A824: 0, #A825: 0, #A826: 0, #A827: 0, #A828: 0, #A829: 0, #A830: 0, #A831: 0, #A832: 0, #A833: 0, #A834: 0, #A835: 0, #A836: 0, #A837: 0, #A838: 0, #A839: 0, #A840: 0, #A841: 0, #A842: 0, #A843: 0, #A844: 0, #A845: 0, #A846: 0, #A847: 0, #A848: 0, #A849: 0, #A850: 0, #A851: 0, #A852: 0, #A853: 0, #A854: 0, #A855: 0, #A856: 0, #A857: 0, #A858: 0, #A859: 0, #A860: 0, #A861: 0, #A862: 0, #A863: 0, #A864: 0, #A865: 0, #A866: 0, #A867: 0, #A868: 0, #A869: 0, #A870: 0, #A871: 0, #A872: 0, #A873: 0, #A874: 0, #A875: 0, #A876: 0, #A877: 0, #A878: 0, #A879: 0, #A880: 0, #A881: 0, #A882: 0, #A883: 0, #A884: 0, #A885: 0, #A886: 0, #A887: 0, #A888: 0, #A889: 0, #A890: 0, #A891: 0, #A892: 0, #A893: 0, #A894: 0, #A895: 0, #A896: 0, #A897: 0, #A898: 0, #A899: 0, #A900: 0, #A901: 0, #A902: 0, #A903: 0, #A904: 0, #A905: 0, #A906: 0, #A907: 0, #A908: 0, #A909: 0, #A910: 0, #A911: 0, #A912: 0, #A913: 0, #A914: 0, #A915: 0, #A916: 0, #A917: 0, #A918: 0, #A919: 0, #A920: 0, #A921: 0, #A922: 0, #A923: 0, #A924: 0, #A925: 0, #A926: 0, #A927: 0, #A928: 0, #A929: 0, #A930: 0, #A931: 0, #A932: 0, #A933: 0, #A934: 0, #A935: 0, #A936: 0, #A937: 0, #A938: 0, #A939: 0, #A940: 0, #A941: 0, #A942: 0, #A943: 0, #A944: 0, #A945: 0, #A946: 0, #A947: 0, #A948: 0, #A949: 0, #A950: 0, #A951: 0, #A952: 0, #A953: 0, #A954: 0, #A955: 0, #A956: 0, #A957: 0, #A958: 0, #A959: 0, #A960: 0, #A961: 0, #A962: 0, #A963: 0, #A964: 0, #A965: 0, #A966: 0, #A967: 0, #A968: 0, #A969: 0, #A970: 0, #A971: 0, #A972: 0, #A973: 0, #A974: 0, #A975: 0, #A976: 0, #A977: 0, #A978: 0, #A979: 0, #A980: 0, #A981: 0, #A982: 0, #A983: 0, #A984: 0, #A985: 0, #A986: 0, #A987: 0, #A988: 0, #A989: 0, #A990: 0, #A991: 0, #A992: 0, #A993: 0, #A994: 0, #A995: 0, #A996: 0, #A997: 0, #A998: 0, #A999: 0, #A1000: 0>

local state explosion

## PRELIMINARIES

**Notation:**  $\mathcal{B}$  = Boolean program,  $pc$  = program counter,  $S$  = set of shared states,  $L = PC \times C$  = set of local states, consisting of program counters  $PC$  and local variable valuations  $C$ .

BWRA operates on WSTS [2]. A WSTS is a transition system equipped with a well quasi-ordering  $\preceq$  on its states that satisfy a monotonicity property.  $\mathcal{B}$  induces a WSTS, with  $\preceq$  defined as follows:

$$\langle s, \{(\ell_1, n_1), \dots, (\ell_k, n_k)\} \rangle \preceq \langle s', \{(\ell'_1, n'_1), \dots, (\ell'_k, n'_k), \dots\} \rangle$$

if  $s = s'$  and  $\forall 1 \leq i \leq k: n_i \leq n'_i$ . We say  $r$  covers  $\tau$  if  $\tau \preceq r$ .

**Definition.** Let  $\uparrow \tau := \{r \mid \tau \preceq r\}$ . Then

$$CovPre(\tau') := \{\tau \mid \exists \tau \rightarrow r, r \in \uparrow \tau'\} \quad \text{and} \\ C-Pre(\tau') := \min\{\tau : \tau \in CovPre(\tau')\}.$$

## REFERENCES

- [1] G. Basler, M. Mazzucchi, T. Wahl, and D. Kroening, "Context-aware counter abstraction," *Form. Methods Syst. Des.*, vol. 36, no. 3, pp. 223–245, Sep. 2010.
- [2] P. A. Abdulla, "Well (and better) quasi-ordered transition systems," *Bulletin of Symbolic Logic*, vol. 16, no. 4, pp. 457–515, 2010.

## CONTRIBUTIONS

In this work, we extend the *context-aware* idea for Boolean programs run by a fixed, finite number of threads [1] to families with *unbounded thread counts*, based on Backward Reachability Analysis (BWRA) [2].

Our main contributions include:

1. performing BWRA **on-the-fly** by operating directly on Boolean programs;
2. avoiding local state explosion with the aid of on-the-fly exploration and efficient ALL-SAT solvers;
3. optimizations to limit the size of obtained covering pre-images.

## EXAMPLE

**C Program**

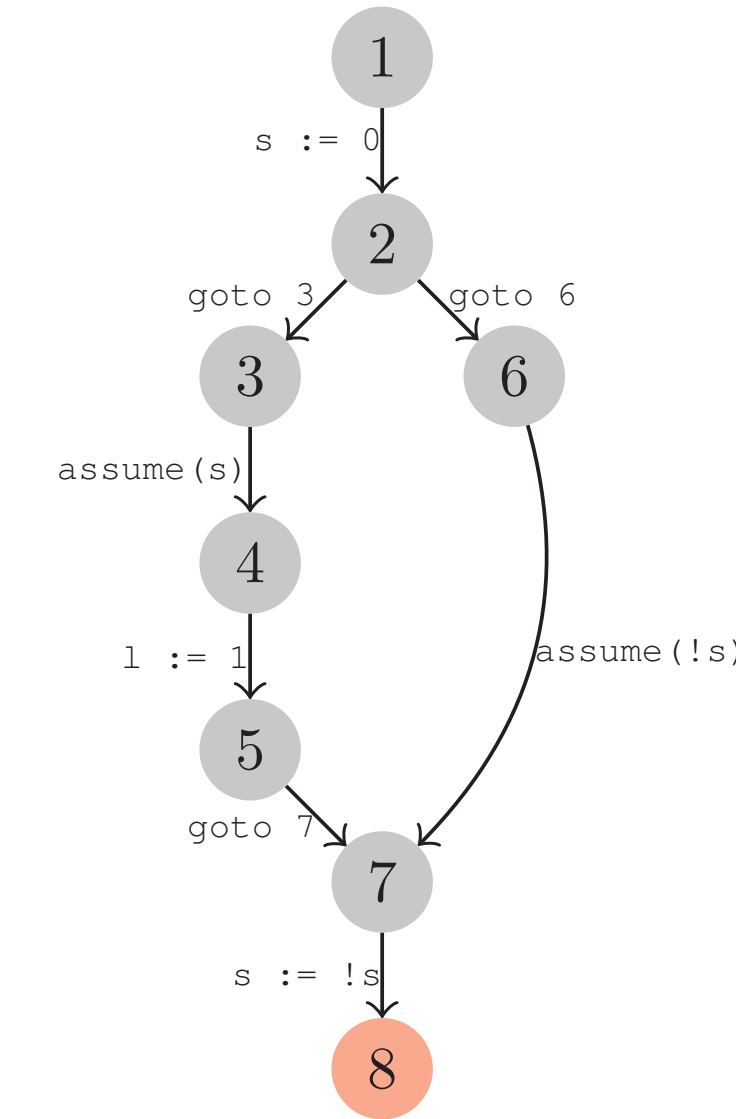
```
int x = 1;
int main() {
  int y = 0;
  x = 0;
  if (x)
    y = 1;
  x = !x;
  assert(!y);
  return 0;
}
```

Predicate Abstraction

**Boolean Program**

```
decl s := 1;
void main() begin
  decl l := 0;
  1: s := 0;
  2: goto 3, 6;
  3: assume(s);
  4: l := 1;
  5: goto 7;
  6: assume(!s);
  7: s := !s;
  8: assert(!l);
end
```

Control Flow Graph of Boolean program



A path explored by on-the-fly BWRA

$s = 0 \wedge l_1 = (1, 8)$   
 $s = 1 \wedge l_1 = (1, 7)$   
 $s = 1 \wedge l_1 = (1, 5)$   
 $s = 1 \wedge l_1 = (\star, 4)$   
 $s = 1 \wedge l_1 = (\star, 3)$   
 $s = 1 \wedge l_1 = (\star, 2)$   
 $s = 1 \wedge l_1 = (\star, 2) \wedge l_2 = (0, 8)$   
 $s = 0 \wedge l_1 = (\star, 2) \wedge l_2 = (0, 7)$   
 $s = 0 \wedge l_1 = (\star, 2) \wedge l_2 = (0, 6)$   
 $s = 0 \wedge l_1 = (\star, 2) \wedge l_2 = (0, 2)$   
 $s = \star \wedge l_1 = (\star, 1) \wedge l_2 = (0, 1)$

$\star$ : nondeterminism; local state  $\ell = (1, 8)$ :  $l = 1 \wedge pc = 8$

## ON-THE-FLY BACKWARD EXPLORATION

**Idea:** compute  $C-Pre(\tau')$  based on *control flow graph* (CFG) and *weakest precondition* (WP) propagation.

1. CFG  $G = (V, E)$ , with  $V$  = set of program locations, and  $E$  = set of execution flows.
2. WP defined as  $WP_{e.stmt}(s, \ell, s', \ell')$ , where  $e.stmt$  is a statement associated with edge  $e \in E$ . It is encoded as a CNF formula, where  $s, \ell$  are free variables, and then input into an ALL-SAT solver.

### Algorithm ON-THE-FLY BW EXPLORATION

**Input:**  $\mathcal{B}$ : a Boolean program with the set of initial thread states  $I$ ;  $\mathcal{T}_{fin}$ : the set of target thread states;  $G=(V, E)$ : a CFG constructed from  $\mathcal{B}$

**Output:** Is  $\uparrow \mathcal{T}_{fin}$  reachable?

- 1:  $\Phi := \mathcal{T}_{fin}$  ▷ the set of unexplored states
- 2:  $\Psi := \emptyset$  ▷ the set of explored states
- 3:  $\Omega := \text{CANDIDATE-LOCAL-STATES}(\mathcal{B})$
- 4: **while**  $\Phi \neq \emptyset$
- 5:   remove  $\tau' = \langle s', Z' \rangle$ , with  $Z$