گزارش فاز دوم – $CheckingModel$ با $SPIN$

پروژه دوم: نظریه زبان‌ها و ماشین‌ها

فاطمه باقریان – امیرحسین پیرنژاد

تیر ۱۴۰۵

فهرست مطالب

۱ مقدمه فاز دوم **۲**

۲ برنامه مورد بررسی **۲**

۳ خصوصیت اول – Safety **۲**
۱.۳ فرمول LTL ۲
۲.۳ دستور اجرا ۲
۳.۳ خروجی ترمینال ۲
۴.۳ تفسیر ۳

۴ خصوصیت دوم – Liveness **۳**
۱.۴ فرمول LTL ۳
۲.۴ دستور اجرا ۳
۳.۴ خروجی ترمینال ۳
۴.۴ تفسیر ۴

۵ خصوصیت سوم – Reachability **۴**
۱.۵ فرمول LTL ۴
۲.۵ دستور اجرا ۴
۳.۵ خروجی ترمینال ۵
۴.۵ تفسیر – باگ :)) ۵

۶ خصوصیت چهارم – Deadlock Freedom **۵**
۱.۶ دستور اجرا ۵
۲.۶ خروجی ترمینال (مسیر اجرای کامل) ۵
۳.۶ تفسیر ۶

۷ خصوصیت پنجم – Invariant **۶**
۱.۷ فرمول LTL ۶
۲.۷ دستور اجرا ۶
۳.۷ خروجی ترمینال ۶
۴.۷ تفسیر ۷

۱ مقدمه فاز دوم

در فاز اول، برنامه‌ی زبان Hash به مدل Promela ترجمه شد (فایل output.pml). هدف این فاز، بررسی پنج خصوصیت مشخص – Safety، Liveness، Reachability، Deadlock Freedom و Invariant – بر روی این مدل با استفاده از ابزار SPIN است. برای هر خصوصیت، فرمول LTL متناظر (در صورت نیاز)، دستور دقیق اجرا، خروجی ترمینال و یک تفسیر مستقل ارائه شده است. تمامی خصوصیات با فرمول‌های named در فایل properties.ltl تعریف شده‌اند و با دستور spin -search -ltl <name> output.pml اجرا شده‌اند.

۲ برنامه مورد بررسی

مدل Promela نهایی (output.pml) شامل یک عملیات تقسیم محافظت‌شده با سازوکار gereftar/emtehan، دو حلقه‌ی متوالی (اولی با شرط i<5، دومی با شرط j<3)، و یک برچسب پایانی endReachedLabel است. متغیرهای کنترلی divByZero، inLoop، exitLoop و endReached برای امکان بیان پنج خصوصیت در سطح سراسری (global) تعریف شده‌اند.

۳ خصوصیت اول – Safety

۱.۳ فرمول LTL

$$\Box \neg(divByZero)$$

۲.۳ دستور اجرا

```
spin -search -ltl safety output.pml
```

۳.۳ خروجی ترمینال

```
(Spin Version 6.5.1 -- 31 July 2020)
+ Partial Order Reduction

Full statespace search for:
never claim             - (none specified)
assertion violations    +
cycle checks            - (disabled by -DSAFETY)
invalid end states      +

State-vector 36 byte, depth reached 68, errors: 0
69 states, stored
0 states, matched
69 transitions (= stored+matched)
0 atomic steps
hash conflicts:         0 (resolved)

Stats on memory usage (in Megabytes):
0.004      equivalent memory usage for states
0.286      actual memory usage for states
```

```
128.000      memory used for hash table (-w24)
0.534      memory used for DFS stack (-m10000)
128.730      total actual memory usage

unreached in proctype main
output.pml:20, state 7,  "divByZero = 1"
output.pml:21, state 8,  "errFlag_1 = 1"
output.pml:29, state 15, "safe = 0"
output.pml:48, state 36, "inLoop = 1"
output.pml:68, state 57, "inLoop = 1"
output.pml:74, state 63, "safe = 0"
(6 of 69 states)

pan: elapsed time 0.12 seconds
pan: rate 575 states/second
```

۴.۳ تفسیر

جستجوی کامل فضای حالت هیچ نقضی برای فرمول $\Box\neg(divByZero)$ پیدا نکرد (errors: 0)، یعنی در تمام ۶۹ حالت قابل‌دسترس، فلگ divByZero هیچ‌گاه مقدار true نگرفته است. با این حال، دقت در بخش unreached in proctype نکته‌ی مهمی را آشکار می‌کند: خط output.pml:20 (یعنی $\text{divByZero} = 1$) اصلاً در فضای حالت کاوش نشده است. علت این است که در مدل، مقدار متغیر y به‌صورت ثابت ($y = 2$) مقداردهی شده و هیچ مسیر اجرایی برای رسیدن y به صفر وجود ندارد.

۴ خصوصیت دوم – Liveness

۱.۴ فرمول LTL

$$\Box\,(inLoop \rightarrow \Diamond\, exitLoop)$$

۲.۴ دستور اجرا

```
spin -search -ltl liveness output.pml
```

۳.۴ خروجی ترمینال

```
(Spin Version 6.5.1 -- 31 July 2020)
+ Partial Order Reduction

Full statespace search for:
never claim             - (none specified)
assertion violations    +
cycle checks            - (disabled by -DSAFETY)
invalid end states      +

State-vector 36 byte, depth reached 68, errors: 0
69 states, stored
```

```
0 states, matched
69 transitions (= stored+matched)
0 atomic steps
hash conflicts:         0 (resolved)

Stats on memory usage (in Megabytes):
0.004      equivalent memory usage for states
0.286      actual memory usage for states
128.000      memory used for hash table (-w24)
0.534      memory used for DFS stack (-m10000)
128.730      total actual memory usage

unreached in proctype main
output.pml:20, state 7,  "divByZero = 1"
output.pml:21, state 8,  "errFlag_1 = 1"
output.pml:29, state 15, "safe = 0"
output.pml:48, state 36, "inLoop = 1"
output.pml:68, state 57, "inLoop = 1"
output.pml:74, state 63, "safe = 0"
(6 of 69 states)

pan: elapsed time 0.504 seconds
pan: rate 136.90 states/second
```

۴.۴ تفسیر

نتیجه نشان می‌دهد errors: 0، یعنی هیچ اجرایی پیدا نشد که در آن inLoop برقرار شود ولی exitLoop هیچ‌وقت به‌دنبالش نیاید. با توجه به اینکه هر دو حلقه‌ی مدل (شرط i<5 و شرط j<3) کراندار (bounded) هستند و همیشه پس از تعداد ثابتی تکرار با break خاتمه می‌یابند، این نتیجه با تحلیل دستی مدل سازگار است: در این برنامه امکان ورود به یک حلقه‌ی بی‌نهایت وجود ندارد.

نکته: در سرتیتر خروجی، عبارت (disabled by -DSAFETY) - cycle checks دیده می‌شود. این یعنی SPIN به‌صورت خودکار تشخیص داده که برای این مدل خاص (که کاملاً deterministic است و هیچ رفتار نامتناهی غیر از توقف نهایی ندارد)، نیازی به جستجوی کامل acceptance cycle در اتوماتای Büchi نیست.(فکر کنم باید تست عوض بشه:))

۵ خصوصیت سوم – Reachability

۱.۵ فرمول LTL

فرمولی که به SPIN داده می‌شود، نقیض فرمول اصلی است:

$$\neg(\Diamond\, endReached)$$

۲.۵ دستور اجرا

```
spin -search -ltl reachability output.pml
```

۳.۵ خروجی ترمینال

```
(Spin Version 6.5.1 -- 31 July 2020)
+ Partial Order Reduction

Full statespace search for:
never claim             - (none specified)
assertion violations    +
cycle checks            - (disabled by -DSAFETY)
invalid end states      +

State-vector 36 byte, depth reached 68, errors: 0
69 states, stored
0 states, matched
69 transitions (= stored+matched)
0 atomic steps
hash conflicts:         0 (resolved)

Stats on memory usage (in Megabytes):
0.004      equivalent memory usage for states
0.286      actual memory usage for states
128.000      memory used for hash table (-w24)
0.534      memory used for DFS stack (-m10000)
128.730      total actual memory usage

unreached in proctype main
output.pml:20, state 7,  "divByZero = 1"
output.pml:21, state 8,  "errFlag_1 = 1"
output.pml:29, state 15, "safe = 0"
output.pml:48, state 36, "inLoop = 1"
output.pml:68, state 57, "inLoop = 1"
output.pml:74, state 63, "safe = 0"
(6 of 69 states)

pan: elapsed time 1.53 seconds
pan: rate 45.09 states/second
```

۴.۵ تفسیر – باگ :))

۶ خصوصیت چهارم – Deadlock Freedom

این خصوصیت نیازی به فرمول LTL ندارد و با قابلیت توکار SPIN بررسی می‌شود.

۱.۶ دستور اجرا

```
spin -search -deadlock output.pml
```

۲.۶ خروجی ترمینال (مسیر اجرای کامل)

```
proctype main
state  1 -> state  2   output.pml:13  x = 10
state  2 -> state  3   output.pml:14  y = 2
state  3 -> state  4   output.pml:15  i = 0
state  4 -> state  5   output.pml:16  safe = 0
state  5 -> state 12   output.pml:18  errFlag_1 = 0
state 12 -> state 11   output.pml:19  else            (y != 0)
state 11 -> state 18   output.pml:24  safe = (x / y)
state 18 -> state 17   output.pml:28  else            (!errFlag_1)
state 17 -> state 20   output.pml:30  (skip)
state 20 -> state 28   output.pml:32  activeLoopCount = activeLoopCount + 1
state 28 -> state 22   output.pml:35  (i < 5)
state 22 -> 23 -> 24 -> 25 -> state 28     ]            [
state 28 -> state 31   output.pml:35  else            (i >= 5)
state 31 -> state 32   output.pml:42  activeLoopCount = activeLoopCount - 1
state 32 -> state 37   output.pml:43  exitLoop = 1
state 37 -> state 34   output.pml:45  (activeLoopCount == 0)
state 34 -> state 39   output.pml:46  inLoop = 0
state 39 -> state 41   output.pml:51  j = 0
state 41 -> state 49   output.pml:52  activeLoopCount = activeLoopCount + 1
state 49 -> state 43   output.pml:54  (j < 3)
state 43 -> 44 -> 45 -> 46 -> state 49     ]            [
state 49 -> state 52   output.pml:54  else            (j >= 3)
state 52 -> state 53   output.pml:62  activeLoopCount = activeLoopCount - 1
state 53 -> state 58   output.pml:63  exitLoop = 1
state 58 -> state 55   output.pml:65  (activeLoopCount == 0)
state 55 -> state 64   output.pml:66  inLoop = 0
state 64 -> state 61   output.pml:71  (x >= 0)
state 61 -> state 66   output.pml:72  safe = safe + 1
state 66 -> state 67   output.pml:76  printf("%d\n", safe)
state 67 -> state 68   output.pml:78  endReached = 1
state 68 -> state 69   output.pml:79  (1)
state 69 -> state  0   output.pml:80  -end-
```

۳.۶ تفسیر

از آنجا که مدل کاملاً deterministic است، SPIN در عمل تنها یک مسیر اجرایی یکتا دارد که به‌طور کامل در بالا نمایش داده شده است. این مسیر بدون هیچ توقف غیرمنتظره‌ای به برچسب -end- می‌رسد، که نشان‌دهنده‌ی یک پایان معتبر (valid end state) است. بنابراین مدل عاری از deadlock است.(هنوز آرمان جواب نداده ولی احتمالا بازم نیازمند تغییر تست)

۷ خصوصیت پنجم – Invariant

۱.۷ فرمول LTL

$$\Box\,(x \geq 0)$$

۲.۷ دستور اجرا

```
spin -search -ltl invariant output.pml
```

۳.۷ خروجی ترمینال

```
(Spin Version 6.5.1 -- 31 July 2020)
+ Partial Order Reduction

Full statespace search for:
never claim             - (none specified)
assertion violations    +
cycle checks            - (disabled by -DSAFETY)
invalid end states      +

State-vector 36 byte, depth reached 68, errors: 0
69 states, stored
0 states, matched
69 transitions (= stored+matched)
0 atomic steps
hash conflicts:         0 (resolved)

Stats on memory usage (in Megabytes):
0.004      equivalent memory usage for states
0.286      actual memory usage for states
128.000      memory used for hash table (-w24)
0.534      memory used for DFS stack (-m10000)
128.730      total actual memory usage

unreached in proctype main
output.pml:20, state 7,  "divByZero = 1"
output.pml:21, state 8,  "errFlag_1 = 1"
output.pml:29, state 15, "safe = 0"
output.pml:48, state 36, "inLoop = 1"
output.pml:68, state 57, "inLoop = 1"
output.pml:74, state 63, "safe = 0"
(6 of 69 states)

pan: elapsed time 0.134 seconds
pan: rate 514.92 states/second
```

۴.۷ تفسیر

جستجوی کامل هیچ حالتی با $x < 0$ پیدا نکرد (errors: 0). این نتیجه با تحلیل دستی مدل سازگار است: متغیر x از مقدار اولیه‌ی ۱۰ شروع می‌شود و تنها در حلقه‌ی اول، دقیقاً ۵ بار یک واحد کاهش می‌یابد (به ازای هر تکرار شرط i<5)؛ بنابراین کمترین مقدار ممکن برای x برابر ۵ است و هیچ‌گاه به صفر یا منفی نمی‌رسد.