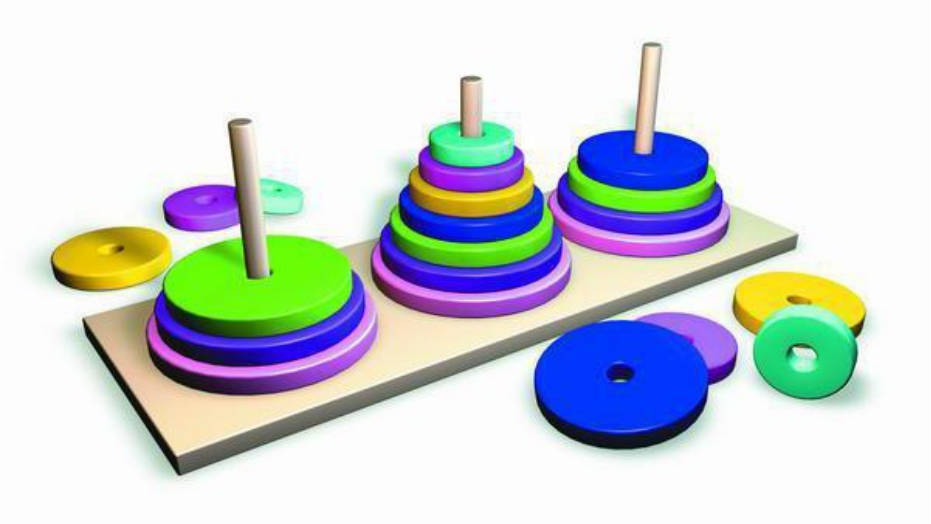
Fehler in Standardsortieralgorithmus mit formalen Methoden aufgedeckt

heise Developer 10.03.2015 08:17 Uhr – Julia Schmidt

vorlesen



Android, Java und Groovy nutzen alle den TimSort-Algorithmus. Informatiker eines Verbundprojekts konnten mit Hilfe eines von ihnen entwickelten Tools nun einen Fehler in der Implementierung feststellen und beheben.

Die Mitglieder eines EU-Verbundprojekts sind beim Testen ihrer Verifikationssoftware KeY auf einen für beseitigt gehaltenen **Fehler im Sortieralgorithmus TimSort** [https://bugs.openjdk.java.net/browse/JDK-8072909] gestoßen. Letzterer kommt unter anderem als Standardmechanismus für Sortieraufgaben im Android SDK, in Suns JDK und OpenJDK zum Einsatz. Die **nun behobene Schwachstelle** [http://www.envisage-project.eu/proving-android-java-and-python-sorting-algorithm-is-broken-and-how-to-fix-it/#sec3] ließ sich wohl theoretisch für Denial-of-Service-Angriffe nutzen, auch wenn die Projektmitarbeiter die akute Bedrohung für gering halten.

Der 2002 von Tim Peters entwickelte Sortieralgorithmus TimSort vereint Ideen aus den Verfahren Merge Sort und Insertion Sort. Er geht den eingegebenen Array von links nach rechts durch und sortiert ihn, indem er aufeinander folgende, disjunkte bereits sortierte Abschnitte aufzufinden versucht, absteigend sortierte Abschnitte umdreht und die Längen der Abschnitte mit einer minimalen Abschnittslänge vergleicht und bei Bedarf auffüllt (**nähere Informationen zur Funktionsweise finden sich in der Beschreibung der ersten Implementierung für Python** [http://bugs.python.org/file4451/timsort.txt]). Die Längen der Abschnitte addiert der Algorithmus und schreibt sie in einen Array *runLen*.

Nach jedem dieser Schreibvorgänge wird eine Methode *mergeCollapse* gestartet, die Abschnitte zusammenführt, bis die letzten drei Elemente in runLen zwei festgelegte Bedingungen erfüllen. Diese Bedingungen geben zusammen eine Invariante. Die Informatiker des Envisage-Projekts konnten nun mit formalen Methoden feststellen, dass die *mergeCollapse*-Methode in bestimmten Fällen gegen die Invariante verstößt und haben **eine Korrektur eingereicht, die für das OpenJDK angenommen wurde** [https://bugs.openjdk.java.net/browse/JDK-8072909] . Eine genaue Beschreibung der Schwachstelle und der formalen Spezifikation der Gegenmaßnahme sind in einem ausführlichen **Blogbeitrag** [http://www.envisage-project.eu/proving-android-java-and-python-sorting-algorithm-is-broken-and-how-to-fix-it/#sec3] beschrieben.

Die zur Verifikation benutzte **KeY-Software** [http://www.key-project.org/download/] des Verbundprojekts, an dem unter anderem das Karlsruhe Institut für Technologie und die Technische Universität Darmstadt beteiligt sind, steht interessierten Entwicklern auf der Projektseite zum Download zur Verfügung. Sie können es unter anderem dazu nutzen, um eigene Programme auf Fehler im Aufbau zu untersuchen. (**jul** [mailto:jul@heise.de])

Kommentare lesen (115 Beiträge)
[http://www.heise.de/forum/heise-Developer/News-Kommentare/Fehler-in-Standardsortieralgorithmus-mit-formalen-Methoden-aufgedeckt/forum-78631/comment/]

Forum bei heise Developer: **Tools** [http://www.heise.de/forum/heise-Developer/Themen-Hilfe/Tools/forum-59941/comment/]

http://heise.de/-2570944 [http://heise.de/-2570944]
Drucken [http://www.heise.de/newsticker/meldung/Fehler-in-Standardsortieralgorithmus-mit-formalen-Methoden-aufgedeckt-2570944.html?view=print]

Mehr zum Thema **Java** [http://www.heise.de/thema/Java] **Python** [http://www.heise.de/thema/Python]

Weitere News zum Thema

Oracle will Java wieder auf Android und iOS bringen

Oracle unterstützt wohl eine mobile Version des OpenJDK, die explizit auf die Plattformen iOS, Android und auch Windows 10 für Mobilgeräte zielt.
01. Oktober 2015, 12:37 Uhr 120

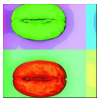
Auftakt der JavaOne 2015: Geburtstagsfeier ohne große Neuigkeiten

Oracle bot während der Eröffnungs-Keynote der weltweit größten Java-Konferenz eine Zusammenfassung dessen, was von Java 9 zu erwarten sein wird und…
26. Oktober 2015, 10:49 Uhr 62

Developer Snapshots: Programmierer-News in ein, zwei Sätzen

heise Developer fasst jede Woche bisher vernachlässigte, aber doch wichtige Nachrichten zu Tools, Spezifikationen oder anderem zusammen – dieses Mal…
17. Juli 2015, 15:02 Uhr

JavaOne 2015: Rundumschlag zum JDK 9



Haben wir nichts anzukündigen, wärmen wir einfach alte Nachrichten auf. So könnte Oracles bisheriges Motto auf der JavaOne 2015 sein. Zumindest stößt…
27. Oktober 2015, 09:26 Uhr 5

Themen im Trend

KIC 8462852: Mysteriöser Stern wird wohl von Kometen umkreist

Schnellspannung

Die Keramik fehlt

Audi quattro concept: Nur eine Studie?