

CoCoA-5 - Bug #1429

Stack overflow reading long list (SEGV)

28 Feb 2020 16:37 - John Abbott

Status:	New	Start date:	28 Feb 2020
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:	enhancing/improving	Estimated time:	0.00 hour
Target version:	CoCoA-5.4.2	Spent time:	1.00 hour

Description

On my computer CoCoAInterpreter generates a SEGV if I give as input a long list, namely

```
L := [  
  1,  
  2,  
  ...  
  550000  
];
```

valgrind reported the problem as a stack overflow (but why?)

The problem was originally reported by Bernhard Andraschko: his computer failed to read a list of about 14400 4x4 matrices. Splitting the list into two separate parts, and then concatenating them worked fine (and quickly).

History

#1 - 28 Feb 2020 16:44 - John Abbott

Yes, of course, inputting explicitly the long list of integers is not commonplace. But it is embarrassing that CoCoA crashed when reading Bernhard's list of 14400 small matrices.

A first guess is that the parser uses a recursive technique to read a long list, and that this triggers a stack overflow. But then why does a list of matrices fail before 14400 elements (on his computer), whereas a list of integers can be much longer -- surely the stack consumption should depend almost solely on the list length...??

The original problem arose when Bernhard wanted to transfer a result from Sage into CoCoA.

The relevant code may be in Parser.C around lines 1771--1779 in the function Parser::parseListPrimary

#2 - 19 Apr 2021 14:14 - John Abbott

- Target version changed from CoCoA-5.4.0 to CoCoA-5.4.2