CoCoA-5 - Bug #189

malloc ERROR

18 Jun 2012 14:32 - Laura Torrente

Status:	Closed	**Start date:**	18 Jun 2012
Priority:	Normal	**Due date:**	
Assignee:	John Abbott	**% Done:**	100%
Category:	Parser/Interpreter	**Estimated time:**	0.00 hour
Target version:	CoCoA-5.0.3	**Spent time:**	5.30 hours

Description

I get the following error

```
CoCoAInterpreter(13411) malloc: *** error for object 0x10156fcb8: incorrect checksum for freed obj
ect - object was probably modified after being freed.
*** set a breakpoint in malloc_error_break to debug
```

I hope it can be fixed soon.

Ciao, Laura

Related issues:

Related to CoCoALib - Bug #190: Subtle ref count bug for poly rings (via Coef...	**Closed**	**19 Jun 2012**

History

#1 - 18 Jun 2012 15:10 - John Abbott

- Assignee set to John Abbott

Recompiled with MemPool debugging and linking with debug_new.o
The problem disappears... this may be enough to let Laura continue for a while.

JAA thinks we'll need valgrind or similar to sort this one out.
Hard to estimate how long it'll take.

#2 - 19 Jun 2012 09:46 - John Abbott

Laura's code works fine on my Linux VM.
However, **Valgrind** confirms that there is a memory access problem (seems to be a pointer/reference to a deleted ring). Will continue to investigate.

#3 - 19 Jun 2012 11:04 - John Abbott

- File genus.cocoa5 added

- File SSE.cocoa5 added

The problem appears to be a **RingHomValue** in the interpreter which has a reference to a CoCoALib **RingHom** which has been destroyed.
Unfortunately everything seems to have a ref count.

Attached are Laura's sources.

#4 - 19 Jun 2012 12:51 - Anna Maria Bigatti

- Category set to Parser/Interpreter

I finally reduced the example: (quite a lot reduced ;-)
it seems due to having both a redefinition of the PolyRing and its CoeffEmbeddingHom

```
For i := 1 To 10 Do
  PrintLn i;
  QQX  := NewPolyRing(QQ, ["x"]);
  phi := CoeffEmbeddingHom(QQX);
EndFor;
```

#5 - 19 Jun 2012 13:47 - John Abbott

According to **valgrind** the following input is enough to do damage:

```
QQx ::= QQ[x];
phi := CoeffEmbeddingHom(QQx);
QQx ::= QQ[x];
```

Time to do some single stepping... sigh!

#6 - 19 Jun 2012 14:06 - John Abbott

Valgrind even complains about the following two lines!!

```
QQx ::= QQ[x];
phi := CoeffEmbeddingHom(QQx);
```

The error happens when the interpreter ends itself.

PS if I continue at this rate, in half an hour I'll have a 0 line program that causes a problem :-)

#7 - 19 Jun 2012 14:33 - John Abbott

- Status changed from New to In Progress

- % Done changed from 0 to 50

If you add

```
phi := 0;
```

after the two lines in my previous post, then the problem goes away!

As far as I can tell, the problem arises inside the dtor for **RuntimeEnvironment**; unfortunately this is "invisible" code.

Even more unfortunately gdb does not work properly in my Linux VM :-(
[or it may just be a consequence of trying to debug invisible code]
So I shall have to try debugging on a real linux box... so I'm putting this issue "on hold" for a little while.

#8 - 19 Jun 2012 16:44 - John Abbott

- Status changed from In Progress to Closed

- % Done changed from 50 to 100

The cause of the problem is a design bug in CoCoALib (see issue #190).
As a consequence I shall close this issue.

The recommended **WORKAROUND** is to assign an innocuous value (*e.g.* 0) to any variable used for holding a RINGHOM value when you have finished using it. Unfortunately, I fear the real bug will be time-consuming to kill. Apologies to all those who have to bespoil their code with the workaround.

#9 - 04 Jul 2012 10:01 - Anna Maria Bigatti

- Target version set to CoCoA-5.0.3

Files

genus.cocoa5	16.1 KB	19 Jun 2012	John Abbott
SSE.cocoa5	5.21 KB	19 Jun 2012	John Abbott