GammaLib - Bug #1065

GModelSpectralNodes::update_flux_cache(void) behavior when zero Nodes

01/08/2014 03:31 PM - Gerard Lucie

Status:	Closed	**Start date:**	01/08/2014
Priority:	Normal	**Due date:**	
Assigned To:	Knödlseder Jürgen	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	00-08-00		

Description

In GModelSpectralNodes when there is zero Nodes:
m_lin_energies.size() and m_values.size() are less then zero,
but m_lin_energies[i+1] and m_values[i+1] in lines 1494 and 1496 are called, leading to a segfault.

I propose adding the following lines before the loop.

```
 if(m_energies.size()<1){
  GException::not_enough_nodes(G_UPDATE_FLUX_CACHE,m_energies.size() );
  }
```

History

#1 - 01/08/2014 05:59 PM - Knödlseder Jürgen

Did this lead to a problem in your case? The loop is

```
 for (int i = 0; i < m_energies.size()-1; ++i) {
```

which should only be entered if the condition i < m_energies.size()-1 is fulfilled. For zero nodes, the right hand side should be -1, hence 0 < -1 is not fulfilled. For one node, the right hand side should be 0, hence 0 < 0 is not fulfilled. The loop is only entered if there are at least 2 nodes, hence there shouldn't be a problem.

#2 - 01/09/2014 01:58 PM - Gerard Lucie

It leads to a segfault. m_energies.size() = 0 but the for loop is still entered. The problem is that m_energies.size() -1 = 18446744073709551615, nonsense because m_energies.size() returns a unsigned int (I guess).
What works for me is to write:

```
for (int i = 0; i < (int)m_energies.size()-1; ++i) {
```

, that is to cast m_energies.size() into an int.

Then you are right throwing an exception before the for loop is not necessary.

#3 - 01/09/2014 02:50 PM - Knödlseder Jürgen

Gerard Lucie wrote:

> It leads to a segfault. m_energies.size() = 0 but the for loop is still entered. The problem is that m_energies.size() -1 = 18446744073709551615, nonsense because m_energies.size() returns a unsigned int (I guess).
> What works for me is to write:
> [...]
> , that is to cast m_energies.size() into an int.
>
> Then you are right throwing an exception before the for loop is not necessary.

Thanks for this fix. Indeed, I have not considered the possibility that m_energies.size() returns a unsigned int.

I'll do the following

```
// Determine number of nodes
int nodes = m_energies.size(); // cast to int as size() returns unsigned
```

```
// Loop over all nodes-1
for (int i = 0; i < nodes-1; ++i) {
```

and push it the trunk.

Once this is done, does this solve the problem or do you get a crash at another point?

#4 - 01/09/2014 03:30 PM - Gerard Lucie

It solves the problem. An exception is thrown later on because the node array is empty, as expected.

#5 - 01/09/2014 03:45 PM - Knödlseder Jürgen

- Status changed from New to Feedback

- Assigned To set to Knödlseder Jürgen

- Target version set to 00-08-00

- % Done changed from 0 to 100

Okay, great. I pushed the above change in devel.

#6 - 02/17/2014 10:17 PM - Knödlseder Jürgen

- Status changed from Feedback to Closed