QGIS Application - Bug report #13366
Crash when adding new field, changing its value and deleting the same field without save

2015-09-15 04:49 PM - Pedro Venâncio

Status:	Closed		
Priority:	Severe/Regression		
Assignee:	Giuseppe Sucameli		
Category:	Vectors		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	21418

Description

QGIS master crashes when adding new field with 'Field calculator' and deleting the same field without save.

This does not happen adding the new field with 'New column'.

Tested with a shapefile in Linux (ubuntu 32bits).

To reproduce:

1) Add a shapefile layer;
2) Open attribute table;
3) Start editing;
4) Open field calculator;
5) Create a new field;
6) Delete column;

Here I get the crash. Backtrace:

```
[New Thread 0x8cd68b40 (LWP 3828)]

Program received signal SIGABRT, Aborted.
0xb76e4d50 in __kernel_vsyscall ()
(gdb) bt
#0  0xb76e4d50 in __kernel_vsyscall ()
#1  0xb206c607 in __GI_raise (sig=sig@entry=6)
    at ../nptl/sysdeps/unix/sysv/linux/raise.c:56
#2  0xb206fa33 in __GI_abort () at abort.c:89
#3  0x080f19fc in myMessageOutput (type=QtFatalMsg,
    msg=0x9db5110 "ASSERT failure in QVector<T>::operator[]: \\"index out of range\\", file /usr/include/qt4/QtCore/qvector.h, line
359")
    at /home/pedro/qgis/QGIS-master/src/app/main.cpp:378
#4  0xb357fc7d in qt_message_output(QtMsgType, char const*) ()
   from /usr/lib/i386-linux-gnu/libQtCore.so.4
#5  0xb3580127 in ?? () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#6  0xb3580658 in qFatal(char const*, ...) ()
   from /usr/lib/i386-linux-gnu/libQtCore.so.4
#7  0xb358071d in qt_assert_x(char const*, char const*, char const*, int) ()
   from /usr/lib/i386-linux-gnu/libQtCore.so.4
#8  0xb4346871 in QVector<QVariant>::operator[] (this=0xbf98e328, i=3)
    at /usr/include/qt4/QtCore/qvector.h:359
```

```
#9  0xb45bd514 in QgsVectorLayerFeatureIterator::updateChangedAttributes (
    this=0xd176040, f=...)
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayerfeatureiterator.cpp:798
#10 0xb45baee6 in QgsVectorLayerFeatureIterator::fetchFeature (this=0xd176040,
    f=...)
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayerfeatureiterator.cpp:235
#11 0xb446968d in QgsAbstractFeatureIterator::nextFeature (this=0xd176040,
    f=...) at /home/pedro/qgis/QGIS-master/src/core/qgsfeatureiterator.cpp:51
#12 0xb3d74ac4 in QgsFeatureIterator::nextFeature (this=0xbf98e3f8, f=...)
    at /home/pedro/qgis/QGIS-master/src/gui/../core/qgsfeatureiterator.h:196
#13 0xb3e08c7e in QgsAttributeTableModel::loadLayer (this=0x9a64708)
    at /home/pedro/qgis/QGIS-master/src/gui/attributetable/qgsattributetablemodel.cpp:367
#14 0xb3fc1689 in QgsAttributeTableModel::qt_static_metacall (_o=0x9a64708,
    _c=QMetaObject::InvokeMetaMethod, _id=3, _a=0xbf98e4f8)
    at /home/pedro/qgis/QGIS-master/build-master/src/gui/attributetable/moc_qgsattributetablemodel.cxx:73
#15 0xb36b20f7 in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#16 0xb4752311 in QgsVectorLayerCache::invalidated (this=0x9c76da8)
    at /home/pedro/qgis/QGIS-master/build-master/src/core/moc_qgsvectorlayercache.cxx:168
#17 0xb45b016f in QgsVectorLayerCache::invalidate (this=0x9c76da8)
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayercache.cpp:266
#18 0xb475201b in QgsVectorLayerCache::qt_static_metacall (_o=0x9c76da8,
    _c=QMetaObject::InvokeMetaMethod, _id=13, _a=0xbf98e618)
    at /home/pedro/qgis/QGIS-master/build-master/src/core/moc_qgsvectorlayercache.cxx:87
#19 0xb36b20f7 in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
#20 0xb4750683 in QgsVectorLayer::updatedFields (this=0xb405cb0)
    at /home/pedro/qgis/QGIS-master/build-master/src/core/moc_qgsvectorlayer.cxx:369
#21 0xb45a1d21 in QgsVectorLayer::updateFields (this=0xb405cb0)
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayer.cpp:2977
#22 0xb45b467c in QgsVectorLayerEditBuffer::updateLayerFields (this=0xb2f9178)
---Type <return> to continue, or q <return> to quit---
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayereditbuffer.cpp:631
#23 0xb45cadde in QgsVectorLayerUndoCommandDeleteAttribute::redo (
    this=0xd282b80)
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayerundocommand.cpp:420
#24 0xb328bed5 in QUndoStack::push(QUndoCommand*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#25 0xb45b2355 in QgsVectorLayerEditBuffer::deleteAttribute (this=0xb2f9178,
    index=3)
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayereditbuffer.cpp:250
#26 0xb459ecae in QgsVectorLayer::deleteAttribute (this=0xb405cb0, index=3)
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayer.cpp:2239
#27 0xb459edbe in QgsVectorLayer::deleteAttributes (this=0xb405cb0, attrs=...)
    at /home/pedro/qgis/QGIS-master/src/core/qgsvectorlayer.cpp:2253
#28 0x08194842 in QgsAttributeTableDialog::on_mRemoveAttribute_clicked (
    this=0x9257000)
    at /home/pedro/qgis/QGIS-master/src/app/qgsattributetabledialog.cpp:720
#29 0x08496193 in QgsAttributeTableDialog::qt_static_metacall (_o=0x9257000,
    _c=QMetaObject::InvokeMetaMethod, _id=13, _a=0xbf98ea18)
    at /home/pedro/qgis/QGIS-master/build-master/src/app/moc_qgsattributetabledialog.cxx:132
#30 0x084965ea in QgsAttributeTableDialog::qt_metacall (this=0x9257000,
    _c=QMetaObject::InvokeMetaMethod, _id=13, _a=0xbf98ea18)
    at /home/pedro/qgis/QGIS-master/build-master/src/app/moc_qgsattributetabledialog.cxx:194
#31 0xb36a3e85 in QMetaObject::metacall(QObject*, QMetaObject::Call, int, void**) () from /usr/lib/i386-linux-gnu/libQtCore.so.4
```

```
#32 0xb36b240d in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
/usr/lib/i386-linux-gnu/libQtCore.so.4
#33 0xb32a626d in QAbstractButton::clicked(bool) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#34 0xb2fc0c21 in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#35 0xb2fc1fa7 in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#36 0xb2fc20ae in QAbstractButton::mouseReleaseEvent(QMouseEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#37 0xb3093977 in QToolButton::mouseReleaseEvent(QMouseEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#38 0xb2c0340a in QWidget::event(QEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#39 0xb2fc30b2 in QAbstractButton::event(QEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#40 0xb3093a64 in QToolButton::event(QEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#41 0xb2ba97f4 in QApplicationPrivate::notify_helper(QObject*, QEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#42 0xb2bb1ea0 in QApplication::notify(QObject*, QEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#43 0xb43cc359 in QgsApplication::notify (this=0xbf98f6c4, receiver=0xb3cb6e8,
    event=0xbf98ef14)
    at /home/pedro/qgis/QGIS-master/src/core/qgsapplication.cpp:255
#44 0xb369ce4a in QCoreApplication::notifyInternal(QObject*, QEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtCore.so.4
#45 0xb2bafb53 in QApplicationPrivate::sendMouseEvent(QWidget*, QMouseEvent*, QWidget*, QWidget*, QWidget**,
QPointer<QWidget>&, bool) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#46 0xb2c337a8 in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
---Type <return> to continue, or q <return> to quit---
#47 0xb2c32ef5 in QApplication::x11ProcessEvent(_XEvent*) ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#48 0xb2c5e554 in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#49 0xb1ab01e3 in g_main_context_dispatch ()
   from /lib/i386-linux-gnu/libglib-2.0.so.0
#50 0xb1ab0468 in ?? () from /lib/i386-linux-gnu/libglib-2.0.so.0
#51 0xb1ab0528 in g_main_context_iteration ()
   from /lib/i386-linux-gnu/libglib-2.0.so.0
#52 0xb36cc95f in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/i386-linux-gnu/libQtCore.so.4
#53 0xb2c5e60e in ?? () from /usr/lib/i386-linux-gnu/libQtGui.so.4
#54 0xb369b823 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/i386-linux-gnu/libQtCore.so.4
#55 0xb369bb49 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) ()
   from /usr/lib/i386-linux-gnu/libQtCore.so.4
#56 0xb36a18fe in QCoreApplication::exec() ()
   from /usr/lib/i386-linux-gnu/libQtCore.so.4
#57 0xb2ba7a24 in QApplication::exec() ()
   from /usr/lib/i386-linux-gnu/libQtGui.so.4
#58 0x080f5b18 in main (argc=1, argv=0xbf98f964)
    at /home/pedro/qgis/QGIS-master/src/app/main.cpp:1212
(gdb) continue
Continuando.
```

[Thread 0x8cd68b40 (LWP 3828) exited]
[Thread 0x922d6b40 (LWP 3774) exited]

Program terminated with signal SIGABRT, Aborted.
The program no longer exists.
(gdb)

Associated revisions

Revision ce626406 - 2015-09-22 01:36 AM - Giuseppe Sucameli

fix crash deleting a new column which contains changed values (fix #13366),

when a column is deleted just rearrange changed attribute map indexes before calling updateLayerFields on the buffer,
otherwise QgsVectorLayerFeatureIterator::updateChangedAttributes will use the changed attribute map with old/wrong indexes

History

#1 - 2015-09-21 01:16 PM - Salvatore Larosa

I can confirm the crash (Debian wheezy) and I am getting a similar crash when deleting a virtual field.
I am attaching the stacktrace here as it seems affecting the same portion of code.

The steps for me are:

- open the attribute table
- create a virtual field with expression = "other field"
- open delete column dialog (from the toolbar of attribute table)
- the only selectable column is the new virtual field, select it
- ok on dialog
- crash

```
Program received signal SIGABRT, Aborted.
0x00007fffefb1e165 in raise () from /lib/x86_64-linux-gnu/libc.so.6
(gdb) bt
#0  0x00007fffefb1e165 in raise () from /lib/x86_64-linux-gnu/libc.so.6
#1  0x00007fffefb213e0 in abort () from /lib/x86_64-linux-gnu/libc.so.6
#2  0x00000000004daa58 in myMessageOutput (type=QtFatalMsg, msg=
    0x6040f58 "ASSERT failure in QVector<T>::remove: \\"index out of range\\", file /usr/include/qt4/QtCore/qvector.h, line 375")
    at /home/sam/pacchetti_gis/QGIS/src/app/main.cpp:378
#3  0x00007ffff2a9e630 in qt_message_output(QtMsgType, char const*) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#4  0x00007ffff2a9ea98 in ?? () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#5  0x00007ffff2a9ec24 in qFatal(char const*, ...) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#6  0x00007ffff3ead1dc in QVector<QVariant>::remove (this=0x7fffffffb7f0, i=2) at /usr/include/qt4/QtCore/qvector.h:375
#7  0x00007ffff3ea8abc in QgsAttributeForm::onAttributeDeleted (this=0x5cd9ad0, idx=2)
    at /home/sam/pacchetti_gis/QGIS/src/gui/qgsattributeform.cpp:295
#8  0x00007ffff3ff48d1 in QgsAttributeForm::qt_static_metacall (_o=0x5cd9ad0, _c=QMetaObject::InvokeMetaMethod, _id=12,
_a=0x7fffffffb9d0)
    at /home/sam/pacchetti_gis/QGIS/build-master/src/gui/moc_qgsattributeform.cxx:87
#9  0x00007ffff2bb954f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#10 0x00007ffff4b3f240 in QgsVectorLayer::attributeDeleted (this=0x5a51640, _t1=2)
    at /home/sam/pacchetti_gis/QGIS/build-master/src/core/moc_qgsvectorlayer.cxx:343
```

#11 0x00007ffff494b0d1 in QgsVectorLayer::removeExpressionField (this=0x5a51640, index=2)
at /home/sam/pacchetti_gis/QGIS/src/core/qgsvectorlayer.cpp:2941
#12 0x00007ffff4947e99 in QgsVectorLayer::deleteAttribute (this=0x5a51640, index=2) at
/home/sam/pacchetti_gis/QGIS/src/core/qgsvectorlayer.cpp:2232
#13 0x00007ffff4948014 in QgsVectorLayer::deleteAttributes (this=0x5a51640, attrs=...)
at /home/sam/pacchetti_gis/QGIS/src/core/qgsvectorlayer.cpp:2253
#14 0x0000000000591e99 in QgsAttributeTableDialog::on_mRemoveAttribute_clicked (this=0x5a265e0)
at /home/sam/pacchetti_gis/QGIS/src/app/qgsattributetabledialog.cpp:725
#15 0x00000000008eb36c in QgsAttributeTableDialog::qt_static_metacall (_o=0x5a265e0, _c=QMetaObject::InvokeMetaMethod, _id=13,
_a=0x7fffffffbec0)
at /home/sam/pacchetti_gis/QGIS/build-master/src/app/moc_qgsattributetabledialog.cxx:133
#16 0x00000000008eb84a in QgsAttributeTableDialog::qt_metacall (this=0x5a265e0, _c=QMetaObject::InvokeMetaMethod, _id=13,
_a=0x7fffffffbec0)
at /home/sam/pacchetti_gis/QGIS/build-master/src/app/moc_qgsattributetabledialog.cxx:195
#17 0x00007ffff2bb9713 in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#18 0x00007ffff25b2f32 in QAbstractButton::clicked(bool) () from /usr/lib/x86_64-linux-gnu/libQtGui.so.4

#2 - 2015-09-21 04:35 PM - Giuseppe Sucameli

- Assignee set to Giuseppe Sucameli
- Status changed from Open to In Progress
- Category changed from Field calculator to Vectors
- Subject changed from Crash when adding new field and deleting the same field without save to Crash when adding new field, changing its value and deleting the same field without save

Even reproducible using "New column", just changing any attribute value of the new column before deleting it.

#3 - 2015-09-21 04:49 PM - Giuseppe Sucameli

- Status changed from In Progress to Closed

Fixed in changeset commit:"ce6264065de0ee4a01f305b411251d65ae54f97f".

#4 - 2015-09-22 12:47 AM - Salvatore Larosa

Hi Giuseppe, so you cannot reproduce the crash with a virtual field following the steps reported in my comment?

Thank you, the first crash (that reported by Pedro) is fixed.

#5 - 2015-09-22 12:59 AM - Giuseppe Sucameli

I overlooked your comment, you are creating a virtual field...
I didn't checked it. Does it still crash with virtual field?

#6 - 2015-09-22 02:40 AM - Salvatore Larosa

Yes, still crash here with commit:ce62640.

#7 - 2015-09-22 06:29 AM - Tom Chadwin

No crash for me on 2.10.1 Win7 x64. Have followed steps here both for normal and virtual field creation, and I've never recreated a crash.