Dyson - Bug #164

JIT does not work in WebKitGTK

2013-12-08 07:15 PM - Igor Pashev

Status:	New	**Start date:**	2013-12-08
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	30%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

http://cgit.osdyson.org/pkg-webkit/webkit.git/

With JIT enabled I can't use JS functions:

```
pashev@bok:~/js$ ./js 'var f = function(x) {return x}; f(0)'
TypeError: function is not a function (evaluating 'f(0)')

pashev@bok:~/js$ ./js 'Math.sin(9)'
0.4121184852417566

g++ -O0 -g js.cpp -o js -I /usr/include/webkitgtk-1.0/JavaScriptCore/ -I /usr/include/webkitgtk-1.
0/ -ljavascriptcoregtk-1.0
```

js.cpp:

```
#include "JSBase.h"
#include "JSObjectRef.h"
#include "JSStringRef.h"
#include "JSContextRef.h"
#include <stdio.h>
#include <stdlib.h>

static const char *progname;
static char buf[1024];

void usage(FILE *out)
{
  fprintf(out, "Usage: %s <js-script>\n", progname);
}

void usageError()
{
  usage(stderr);
  exit(1);
}

static void evaluate(const char *text)
{
  JSGlobalContextRef context = JSGlobalContextCreateInGroup(NULL, NULL);
  JSValueRef exception;
  JSStringRef script = JSStringCreateWithUTF8CString(text);
  JSValueRef result = JSEvaluateScript(context, script, NULL, NULL, 1, &exception);
  if (result)
    {
      JSStringRef str = JSValueToStringCopy(context, result, NULL);
      (void) JSStringGetUTF8CString(str, buf, sizeof(buf));
      printf("%s\n", buf);
    }
  else
    {
```

```
      JSStringRef exceptionIString = JSValueToStringCopy(context, exception, NULL);
      size_t exceptionUTF8Size = JSStringGetMaximumUTF8CStringSize(exceptionIString);
      char* exceptionUTF8 = (char*)malloc(exceptionUTF8Size);
      JSStringGetUTF8CString(exceptionIString, exceptionUTF8, exceptionUTF8Size);
      printf("%s\n", exceptionUTF8);
      free(exceptionUTF8);
      JSStringRelease(exceptionIString);
    }
}

int main(int argc, char* argv[])
{
  progname = argv[0];
  if (argc != 2)
    usageError();
  evaluate(argv[1]);
  return 0;
}
```

Related issues:

Related to Dyson - Bug #160: QScriptEngine fails to create function objects	**Closed**	**2013-10-27**

History

#1 - 2013-12-08 07:31 PM - Igor Pashev

- Description updated

#2 - 2013-12-16 06:54 PM - Igor Pashev

- Status changed from New to In Progress

- % Done changed from 0 to 30

Partially fixed: only LLint with C;
http://cgit.osdyson.org/pkg-webkit/webkit.git/tree/debian/patches/dyson-solaris-amd64-memory-layout.patch?h=unstable&id=1b953db37a2cac28b465449e2441be4453243998

#3 - 2014-10-19 10:15 PM - Igor Pashev

- Status changed from In Progress to New