UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

Memory consumption of QtWebKit under Linux

Zoltán Herczeg

University of Szeged

Memory measurement methods

OS-based

- Maximum Resident Set Size
  - 4Kb pages allocated for a program
  - Both exclusive and non-exclusive pages
    - Non-exclusive: code pages, shared-data pages
- Advantages
  - Total system memory consumption
- Disadvantages
  - Allocation source unknown
    - Not suitable for optimizations

Getting malloc statistics

- The system malloc has some statistical functions about total memory consumption
- Advantages
  - Really fast
  - Memory consumption in bytes
- Disadvantages
  - mmap regions cannot be measured
  - Call-stack not available

Compiler-based

- Overloading new and delete operators, and using custom allocators or using preprocessor directives
- One step furter than malloc statistics
  - The position (file and line) of the allocation can be recorded
  - Slight performance overhead
  - Cannot measure the the memory consumption of system libraries

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

New tool for valgrind: freya

What else can we do?

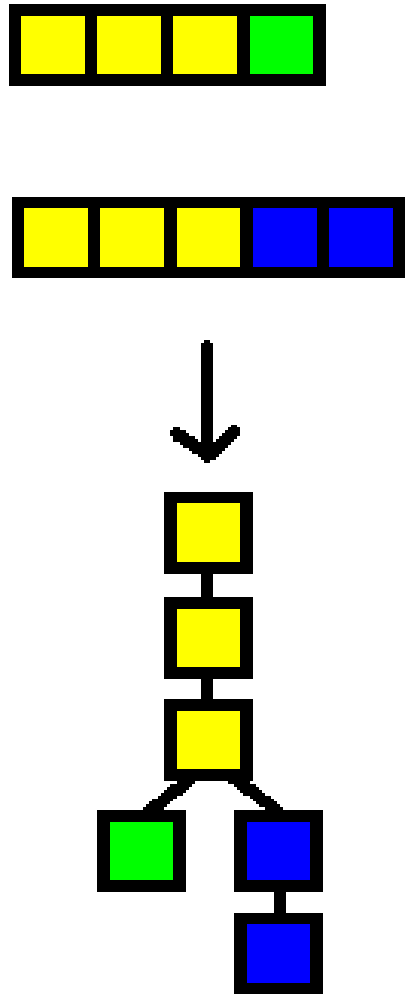
- Valgrind, the JIT engine
  - Recompiles binary executables
    - Dynamic code modification is possible (mainly inserting extra function calls).
  - Huge performance overhead
    - Cannot be used for performance analysis
- We can capture all mallocs and mmaps
  - Stack trace is available

Freya special features

- Can track mmap'ed regions
  - Capturing all memory writes
  - Real allocation
- Unique feature: organizing results
  - Using custom configuration files
  - Can remove the unwanted allocation calls from the top of the stack trace

Freya special features (2)

- The stack traces stored in a tree
  - The common parts of the traces are joined together
- The tree nodes collects
  - the total and peak memory consumption values
  - Number of allocations



Results

Comparing Qt 4.6 and 4.5.3

Name		4.6.0	4.5.3	(%)
www.google.com	Qt	1.1Mb	2.4Mb	54%
	Wk	1.0Mb	1.1Mb	9%
	All	3.8Mb	5.6Mb	32%
www.myspace.com	Qt	10.0Mb	12.7Mb	21%
	Wk	4.7Mb	4.9Mb	4%
	All	15.0Mb	18.6Mb	19%
www.youtube.com	Qt	3.3Mb	5.7Mb	42%
	Wk	3.7Mb	3.7Mb	0%
	All	7.6Mb	11.7Mb	35%

Comparing Qt 4.6 and 4.5.3

Name		4.6.0	4.5.3	(%)
www.ebay.com	Qt	4.1Mb	5.3Mb	23%
	Wk	5.2Mb	5.5Mb	5%
	All	10.7Mb	12.4Mb	14%
en.wikipedia.org/ wiki/Webkit	Qt	4.3Mb	5.7Mb	25%
	Wk	5.2Mb	5.5Mb	5%
	All	10.7Mb	12.5Mb	14%
maps.google.com	Qt	1.4Mb	3.5Mb	60%
	Wk	6.1Mb	6.1Mb	0%
	All	9.0Mb	11.5Mb	22%

Patches

- Bug 31930: 270k allocated instead of 32 byte (!)
  - Landed (r51457)
- Bug 44309: String::append should not duplicate strings, if the right side is empty.
  - Landed (r51705)

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

Big memory contributors

- Cached scripts
  - Many pages put all their JS code together in one file, and we must cache the whole file.
- JavaScriptCore
  - Allocates 270k blocks for internal heap, easly reach > 1M consumption
    - Garbage collected areas
- Images