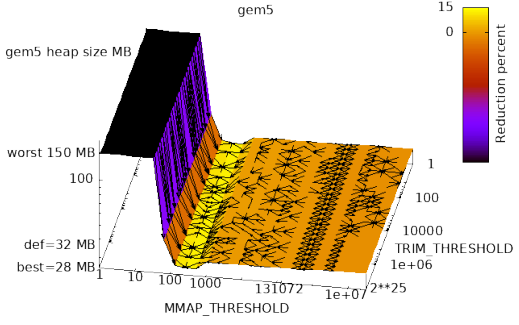
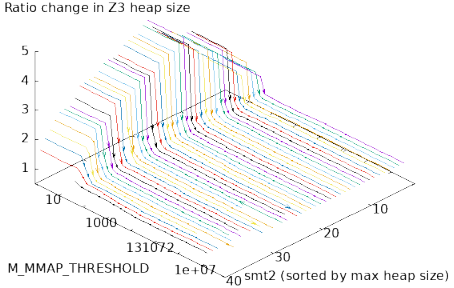
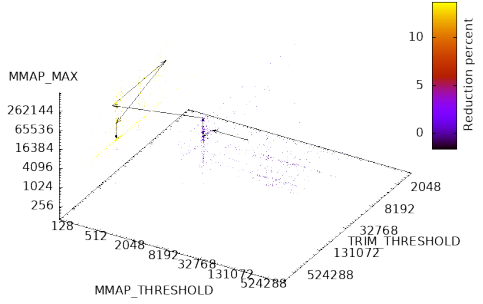
gem5/Z3/gcc/Clang/Redis Heap Fitness Landscapes
Evo* 2025 Late-Breaking Abstracts

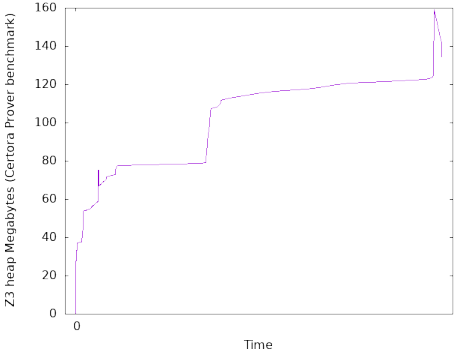
William.B. Langdon, Justyna Petke, David Clark Department of Computer Science, UCL

We adapt “The gem5 C++ glibc Heap Fitness Landscape" W.B. Langdon and B.R. Bruce GI@ICSE 2025”, to use Valgrind Massif on 1,300,000 line C++ gem5, on Microsoft’s 600,000 LOC C++ theorem prover Z3 and benchmarks from the SMT-COMP 2024. Showing the memory landscape is far smoother than is commonly assumed and that Magpie and CMA-ES can tune GNU malloc giving 2.4 megabytes reductions in peak RAM use without coding changes. Similar results are given on the GCC and Clang LLVM compilers and 150,000 LOC C Redis key-value database.





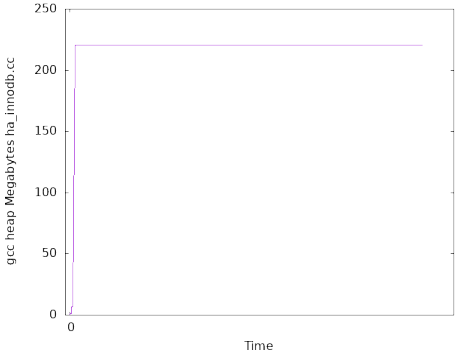


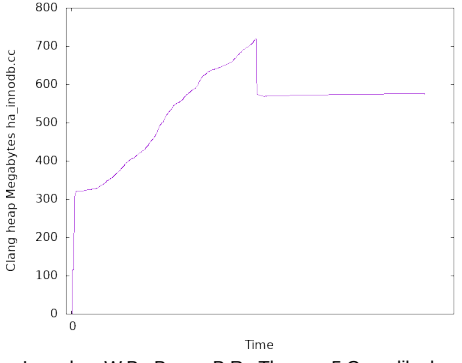


M_MMAP_MAX_tune	g[0,33554432,1/65536][65536]
M_TRIM_THRESHOLD_tune	g[0,33554432,1/131072][131072]
M_MMAP_THRESHOLD_tune	g[0,33554432,1/131072][131072]

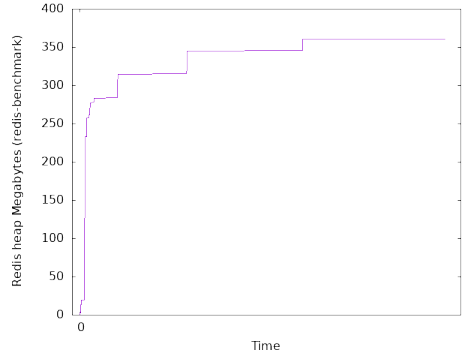
Table 2. Mean percentage improvement of ten runs of Magpie and CMA-ES

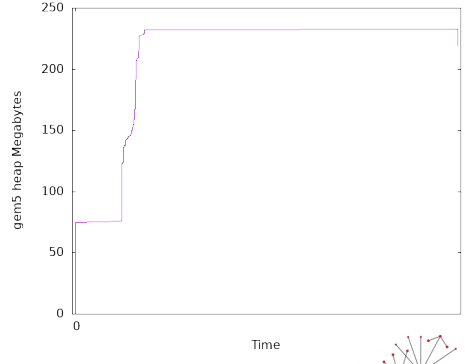
	Z3	(best)	gcc	(best)	Clang	(best)	Redis	(best)
Magpie	1.5 ± 0.0	1.5	0.0 ± 0.0	0.0	0.0 ± 0.0	0.1	0.3 ± 0.0	0.3
CMA-ES	1.5 ± 0.0	1.5	0.0 ± 0.0	0.0	0.0 ± 0.0	0.0	0.2 ± 0.1	0.3



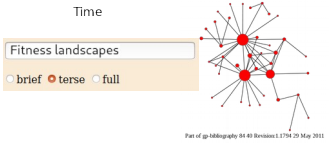


1. Langdon, W.B., Bruce, B.R.: The gem5 C++ glibc heap fitness landscape. In: GI @ICSE 2025. (27 Apr 2025)
2. Blot, A., Petke, J.: Empirical comparison of search heuristics for genetic improvement of software. IEEE TEVC 25(5), 1001-1011 (Oct 2021)
3. Bruce, B.R.: The Blind Software Engineer: Improving The Non-Functional Properties of Software by Means of Genetic Improvement. Ph.D. thesis, UCL, UK (2018)
4. Mesecan, I., et al.: HyperGI: Automated detection and repair of information flow leakage. In: ASE NIER 2021.





COW 67
30 June - 1 July
2025, AI&SE



w.langdon@cs.ucl.ac.uk
j.petke@ucl.ac.uk
david.clark@ucl.ac.uk