Make out like a (Multi-Armed) Bandit: Improving the Odds of Fuzzer Seed Scheduling with T-Scheduler

Anonymous Author(s)*

ACM Reference Format:
Anonymous Author(s). 2023. Make out like a (Multi-Armed) Bandit: Improving the Odds of Fuzzer Seed Scheduling with T-Scheduler. In *Proceedings of 46th International Conference on Software Engineering (ICSE 2024).* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

REFERENCES

[1] Andrea Arcuri and Lionel Briand. 2011. A Practical Guide for Using Statistical Tests to Assess Randomized Algorithms in Software Engineering. In *International Conference on Software Engineering (ICSE).* ACM, 1–10. https://doi.org/10.1145/1985793.1985795

[2] Ahmad Hazimeh, Adrian Herrera, and Mathias Payer. 2020. Magma: A Ground-Truth Fuzzing Benchmark. *Measurement and Analysis of Computing Systems* 4, 3, Article 49 (2020), 29 pages. https://doi.org/10.1145/3428334

[3] Adrian Herrera, Hendra Gunadi, Shane Magrath, Michael Norrish, Mathias Payer, and Antony L. Hosking. 2021. Seed Selection for Successful Fuzzing. In *International Symposium on Software Testing and Analysis (ISSTA).* ACM, 230–243. https://doi.org/10.1145/3460319.3464795

[4] Adrian Herrera, Mathias Payer, and Antony L. Hosking. 2022. Registered Report: datAFLow Towards a Data-Flow-Guided Fuzzer. In *Fuzzing Workshop (FUZZING).* The Internet Society, 11 pages. https://doi.org/10.14722/fuzzing.2022.23001

[5] Nathan Mantel. 1966. Evaluation of survival data and two new rank order statistics arising in its consideration. *Cancer Chemotherapy Reports* 50, 3 (1966), 163–170.

[6] Jonas Benedict Wagner. 2017. *Elastic Program Transformations: Automatically Optimizing the Reliability/Performance Trade-off in Systems Software.* Ph. D. Dissertation. EPFL. https://doi.org/10.5075/epfl-thesis-7745

A MAGMA SURVIVAL ANALYSIS

Following prior work [1–4, 6], we model bug finding using survival analysis. This allows us to reason about censored data; i.e., the case where a fuzzer does not find a bug. Table 1 presents the restricted mean survival time (RMST) of a given bug; i.e., the mean time the bug "survives" being discovered by a fuzzer across ten repeated 72 h campaigns. Lower RMSTs imply a fuzzer finds a bug "faster", while a smaller confidence interval (CI) means the bug is found more consistently. Applying the log-rank test [5] under the null hypothesis that two fuzzers share the same survival function allows us to statistically compare survival times. Thus, two fuzzers have statistically equivalent bug survival times if the log-rank test's p-value > 0.05. The survival analysis results in Table 1 augment those presented in **??**.

B SCHEDULER OVERHEAD

Table 2 shows the per-target scheduler overheads for the 19 FuzzBench targets summarized in Table 3.

ICSE 2024, April 2024, Lisbon, Portugal

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

B.1 Scheduler Overheads

Table 1: Magma bugs triggered, presented as the restricted mean survival time (RMST; in hours) with 95 % bootstrap CI. Bugs never found by a particular fuzzer have an RMST of ⊤ (to distinguish bugs with a 72 h RMST). Targets that fail to build with a given fuzzer are marked with ✗. The best-performing fuzzer (fuzzers if the bug survival times are statistically equivalent per the log-rank test) for each bug is highlighted in green (smaller is better).

Target	Driver	Bug	Fuzzer												
			AFL++								K-Sched	Tortoise	T-Scheduler		
			EXPLORE	FAST	COE	QUAD	LIN	EXPLOIT	MMOPT	RARE			RARE⁻	RARE⁺	SAMPLE
libpng	libpng_read_fuzzer	PNG001	71.51 ± 1.67	⊤	⊤	⊤	⊤	70.53 ± 5.00	⊤	⊤	⊤	⊤	⊤	⊤	⊤
		PNG003	14.40 ± 25.24	0.01 ± 0.00	0.01 ± 0.01	7.21 ± 14.11	28.80 ± 30.92	0.01 ± 0.01	7.21 ± 18.93	7.21 ± 17.28	0.01 ± 0.01	0.01 ± 0.01	0.01 ± 0.01	0.01 ± 0.01	0.01 ± 0.01
		PNG006	14.45 ± 17.84	0.08 ± 0.05	0.04 ± 0.02	7.24 ± 12.76	28.83 ± 24.43	0.05 ± 0.03	7.25 ± 12.75	7.26 ± 12.75	⊤	⊤	⊤	⊤	⊤
		PNG007	39.28 ± 19.37	35.25 ± 13.41	51.15 ± 19.63	38.13 ± 21.00	47.51 ± 20.87	26.85 ± 14.18	42.04 ± 19.27	52.84 ± 18.18	68.36 ± 12.35	70.22 ± 6.03	28.31 ± 15.21	30.63 ± 14.04	28.02 ± 16.30
libsndfile	sndfile_fuzzer	SND001	0.64 ± 0.24	0.41 ± 0.11	0.46 ± 0.21	1.29 ± 0.52	1.43 ± 0.31	2.46 ± 1.64	0.56 ± 0.36	0.45 ± 0.17	34.02 ± 0.53	⊤	0.24 ± 0.08	0.21 ± 0.11	0.32 ± 0.08
		SND005	0.97 ± 0.27	0.78 ± 0.32	1.09 ± 0.42	3.92 ± 1.48	2.88 ± 1.07	6.57 ± 3.59	1.51 ± 0.68	1.02 ± 0.43	⊤	2.82 ± 1.20	0.41 ± 0.10	0.55 ± 0.24	0.48 ± 0.13
		SND006	1.11 ± 0.86	1.10 ± 1.23	0.85 ± 0.51	0.98 ± 0.46	5.69 ± 7.29	6.36 ± 2.68	1.00 ± 0.44	0.34 ± 0.14	68.24 ± 12.76	⊤	0.40 ± 0.14	0.45 ± 0.19	0.36 ± 0.08
		SND007	0.70 ± 0.32	0.85 ± 0.30	0.46 ± 0.27	1.27 ± 0.53	1.57 ± 0.61	2.86 ± 1.42	1.27 ± 0.56	0.66 ± 0.27	56.23 ± 15.46	⊤	0.60 ± 0.26	0.80 ± 0.18	0.79 ± 0.31
		SND017	0.34 ± 0.19	0.47 ± 0.31	0.57 ± 0.23	0.89 ± 0.69	1.67 ± 1.19	0.59 ± 0.15	0.57 ± 0.20	0.74 ± 0.41	1.94 ± 0.12	0.67 ± 0.13	1.35 ± 0.90	0.36 ± 0.31	0.34 ± 0.22
		SND020	0.75 ± 0.30	0.80 ± 0.29	1.06 ± 0.21	1.40 ± 0.49	2.18 ± 0.83	2.03 ± 0.74	1.12 ± 0.25	1.14 ± 0.27	⊤	⊤	2.96 ± 0.93	3.36 ± 1.52	2.63 ± 0.96
		SND024	0.59 ± 0.27	0.38 ± 0.27	0.30 ± 0.14	0.98 ± 0.46	0.93 ± 0.37	2.62 ± 1.27	0.97 ± 0.43	0.34 ± 0.14	60.41 ± 15.52	⊤	0.38 ± 0.15	0.45 ± 0.19	0.35 ± 0.08
libtiff	tiff_read_rgba_fuzzer	TIF002	60.02 ± 15.10	60.46 ± 18.66	60.19 ± 10.33	65.84 ± 20.91	66.72 ± 11.50	62.47 ± 14.48	56.93 ± 15.73	58.95 ± 17.79	⊤	⊤	58.99 ± 13.38	66.96 ± 8.80	64.17 ± 12.92
		TIF007	0.07 ± 0.04	0.08 ± 0.03	0.04 ± 0.02	0.12 ± 0.14	0.06 ± 0.03	0.05 ± 0.02	0.03 ± 0.02	0.04 ± 0.03	1.66 ± 0.40	4.45 ± 1.58	0.03 ± 0.02	0.04 ± 0.03	0.02 ± 0.01
		TIF008	67.16 ± 9.80	64.98 ± 23.84	⊤	⊤	⊤	66.81 ± 11.22	63.17 ± 17.41	67.89 ± 13.95	⊤	⊤	66.63 ± 14.58	⊤	64.90 ± 14.50
		TIF012	1.52 ± 0.56	1.92 ± 1.01	1.25 ± 0.34	3.05 ± 1.04	1.75 ± 0.35	1.44 ± 0.72	1.35 ± 0.36	1.84 ± 0.49	2.42 ± 0.54	51.10 ± 18.80	1.37 ± 0.66	0.97 ± 0.34	0.90 ± 0.39
		TIF014	5.63 ± 2.44	2.72 ± 1.17	4.17 ± 1.69	4.12 ± 2.89	3.11 ± 2.39	2.49 ± 1.27	3.68 ± 2.52	1.59 ± 0.65	⊤	64.30 ± 19.23	2.15 ± 1.41	3.85 ± 2.27	2.04 ± 0.98
	tiffcp	TIF002	⊤	68.29 ± 12.58	⊤	⊤	⊤	69.71 ± 7.78	70.72 ± 4.35	66.34 ± 10.97	⊤	⊤	65.47 ± 15.84	⊤	66.71 ± 10.45
		TIF005	69.44 ± 8.68	65.94 ± 20.57	65.84 ± 20.90	⊤	61.04 ± 22.01	66.74 ± 10.31	⊤	⊤	⊤	⊤	68.74 ± 11.05	⊤	⊤
		TIF006	22.19 ± 8.76	22.62 ± 13.97	13.46 ± 5.32	51.00 ± 17.15	46.21 ± 22.09	31.89 ± 14.87	16.42 ± 13.61	12.05 ± 4.82	64.89 ± 24.15	41.90 ± 17.22	14.92 ± 7.82	20.82 ± 12.40	20.53 ± 9.97
		TIF007	0.05 ± 0.03	0.06 ± 0.03	0.17 ± 0.16	0.14 ± 0.09	0.05 ± 0.03	0.07 ± 0.04	0.05 ± 0.03	0.05 ± 0.03	0.23 ± 0.11	9.52 ± 2.80	0.04 ± 0.02	0.04 ± 0.03	0.03 ± 0.02
		TIF008	65.04 ± 23.61	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤
		TIF009	28.49 ± 19.49	30.93 ± 20.82	25.45 ± 19.99	37.69 ± 17.37	33.09 ± 22.14	23.03 ± 18.04	18.79 ± 11.26	19.39 ± 14.14	3.29 ± 2.11	10.62 ± 1.53	14.31 ± 3.47	33.37 ± 15.03	33.77 ± 17.58
		TIF012	1.26 ± 0.30	0.86 ± 0.31	1.33 ± 0.51	7.77 ± 5.61	2.41 ± 1.05	1.36 ± 0.45	0.89 ± 0.22	1.37 ± 0.57	7.30 ± 5.82	54.88 ± 15.72	2.43 ± 0.99	1.53 ± 0.79	1.15 ± 0.39
		TIF014	4.06 ± 1.99	3.18 ± 1.49	1.80 ± 0.60	9.53 ± 7.82	3.93 ± 2.29	2.48 ± 1.06	1.32 ± 0.43	1.05 ± 0.33	5.68 ± 2.66	61.01 ± 15.90	1.29 ± 0.61	0.93 ± 0.44	0.87 ± 0.39

Table 1: Magma bugs (cont.).

Target	Driver	Bug	Fuzzer												
			AFL++								K-Sched	Tortoise	T-Scheduler		
			EXPLORE	FAST	COE	QUAD	LIN	EXPLOIT	MMOPT	RARE			Rare⁻	Rare⁺	Sample
libxml2	`xml_read_memory_fuzzer`	XML001	⊤	⊤	67.43 ± 8.15	⊤	⊤	⊤	43.49 ± 14.41	⊤	⊤	⊤	⊤	65.80 ± 8.42	65.02 ± 13.91
		XML002	⊤	⊤	⊤	⊤	71.33 ± 2.27	⊤	65.73 ± 21.28	67.52 ± 15.20	⊤	⊤	⊤	68.72 ± 11.15	61.70 ± 20.67
		XML003	5.49 ± 2.49	2.78 ± 2.09	2.59 ± 0.92	1.94 ± 1.16	2.63 ± 0.80	8.58 ± 5.46	9.29 ± 12.41	3.58 ± 1.82	⊤	⊤	4.93 ± 2.74	1.69 ± 0.83	2.84 ± 1.21
		XML009	1.11 ± 0.23	1.52 ± 0.48	1.43 ± 0.46	2.45 ± 0.92	5.16 ± 2.16	4.83 ± 1.73	8.16 ± 12.59	1.82 ± 0.88	⊤	⊤	1.55 ± 0.90	1.64 ± 0.91	1.20 ± 0.46
		XML012	69.16 ± 9.65	60.42 ± 11.63	70.18 ± 6.19	⊤	63.83 ± 12.93	⊤	48.18 ± 18.08	⊤	⊤	⊤	⊤	⊤	71.61 ± 1.33
		XML017	0.02 ± 0.02	0.02 ± 0.02	0.02 ± 0.02	0.04 ± 0.06	0.06 ± 0.04	0.02 ± 0.02	7.21 ± 16.00	0.03 ± 0.02	0.02 ± 0.02	0.03 ± 0.03	0.02 ± 0.02	0.02 ± 0.01	0.03 ± 0.02
	`xmllint`	XML001	58.72 ± 11.70	62.41 ± 9.50	63.36 ± 7.42	68.58 ± 11.62	60.06 ± 16.06	⊤	54.85 ± 11.93	65.02 ± 10.46	⊤	⊤	62.34 ± 8.09	52.02 ± 11.68	57.17 ± 8.30
		XML002	65.11 ± 14.82	71.07 ± 3.16	68.13 ± 13.14	⊤	66.00 ± 20.38	⊤	⊤	66.75 ± 17.82	⊤	⊤	69.56 ± 8.29	66.25 ± 11.28	65.02 ± 23.70
		XML009	1.47 ± 0.72	2.03 ± 0.92	2.01 ± 0.80	5.89 ± 2.55	6.37 ± 2.64	6.17 ± 2.18	2.30 ± 1.27	2.70 ± 1.53	66.68 ± 9.16	⊤	1.11 ± 0.40	0.93 ± 0.46	0.64 ± 0.21
		XML012	⊤	⊤	65.92 ± 12.90	65.67 ± 21.48	66.99 ± 17.02	⊤	65.99 ± 20.39	⊤	⊤	⊤	⊤	⊤	67.14 ± 14.06
		XML017	0.03 ± 0.02	0.05 ± 0.05	0.04 ± 0.03	0.07 ± 0.07	0.06 ± 0.04	0.02 ± 0.02	0.03 ± 0.02	0.02 ± 0.02	0.01 ± 0.02	0.13 ± 0.09	0.04 ± 0.03	0.03 ± 0.02	0.03 ± 0.02
lua	`lua`	LUA002	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	67.10 ± 6.58	69.76 ± 7.61	71.10 ± 3.04
		LUA004	5.68 ± 2.17	8.15 ± 2.27	5.75 ± 2.87	14.95 ± 5.97	36.47 ± 20.63	35.36 ± 9.31	5.89 ± 3.57	10.19 ± 4.25	9.93 ± 4.11	7.21 ± 17.28	9.69 ± 2.90	6.24 ± 2.08	10.03 ± 2.58
openssl	`asn1`	SSL001	35.11 ± 12.55	25.39 ± 7.22	28.46 ± 9.54	44.71 ± 11.97	47.63 ± 13.78	8.58 ± 3.50	19.74 ± 6.45	38.69 ± 9.26	66.85 ± 17.47	⊤	5.72 ± 2.27	5.45 ± 2.84	6.53 ± 3.68
		SSL003	0.06 ± 0.07	0.06 ± 0.06	0.06 ± 0.06	0.06 ± 0.06	0.06 ± 0.06	0.06 ± 0.05	0.06 ± 0.05	0.06 ± 0.05	0.16 ± 0.00	0.26 ± 0.00	0.06 ± 0.04	0.07 ± 0.08	0.07 ± 0.07
	`client`	SSL002	0.08 ± 0.06	0.17 ± 0.20	0.07 ± 0.05	0.08 ± 0.06	0.08 ± 0.06	0.08 ± 0.05	0.07 ± 0.05	0.08 ± 0.05	0.17 ± 0.00	50.42 ± 37.31	0.09 ± 0.08	0.08 ± 0.06	0.09 ± 0.06
	`server`	SSL002	0.11 ± 0.08	0.11 ± 0.08	0.12 ± 0.08	0.16 ± 0.09	0.11 ± 0.08	0.12 ± 0.08	0.16 ± 0.09	0.11 ± 0.08	0.22 ± 0.00	0.35 ± 0.00	0.11 ± 0.08	0.11 ± 0.08	0.12 ± 0.09
		SSL020	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	18.62 ± 4.02	16.42 ± 3.27	29.93 ± 16.92	37.10 ± 14.20	46.80 ± 16.06
	`x509`	SSL009	⊤	71.49 ± 1.74	66.82 ± 17.60	⊤	⊤	64.89 ± 12.55	⊤	54.42 ± 19.80	⊤	27.31 ± 17.28	⊤	⊤	⊤
php	`exif`	PHP004	57.62 ± 28.19	70.00 ± 6.80	49.60 ± 23.07	57.61 ± 28.20	⊤	48.32 ± 16.34	65.14 ± 23.29	51.48 ± 27.52	✗	2.77 ± 0.06	5.61 ± 3.11	5.48 ± 5.15	2.88 ± 2.54
		PHP009	56.61 ± 17.72	30.29 ± 17.40	49.65 ± 24.01	68.83 ± 8.99	61.50 ± 14.04	15.25 ± 7.36	27.63 ± 19.74	33.01 ± 20.78	✗	3.51 ± 0.22	1.22 ± 0.76	0.64 ± 0.28	0.98 ± 0.57
		PHP011	2.55 ± 1.37	1.67 ± 1.89	3.16 ± 2.88	1.54 ± 1.14	3.80 ± 3.16	0.70 ± 0.41	1.42 ± 1.03	1.11 ± 0.94	✗	2.23 ± 0.03	0.13 ± 0.06	0.21 ± 0.07	0.22 ± 0.09

Table 1: Magma bugs (cont.).

Target	Driver	Bug	Fuzzer												
			AFL++								K-Sched	Tortoise	T-Scheduler		
			EXPLORE	FAST	COE	QUAD	LIN	EXPLOIT	MMOPT	RARE			RARE$^-$	RARE$^+$	SAMPLE
poppler	pdf_fuzzer	PDF001	⊤	65.08 ± 23.48	⊤	⊤	⊤	⊤	⊤	⊤	✗	⊤	⊤	⊤	⊤
		PDF010	1.15 ± 0.53	1.82 ± 0.50	1.89 ± 1.34	5.25 ± 2.81	5.63 ± 2.40	2.07 ± 2.03	1.96 ± 1.22	1.61 ± 0.56	✗	0.10 ± 0.10	0.99 ± 0.47	1.23 ± 0.52	1.24 ± 0.69
		PDF011	65.59 ± 21.76	⊤	66.53 ± 18.57	60.79 ± 21.97	⊤	65.88 ± 20.79	⊤	⊤	✗	⊤	67.01 ± 12.96	65.70 ± 21.39	55.79 ± 21.95
		PDF016	0.04 ± 0.02	0.05 ± 0.03	0.06 ± 0.04	0.07 ± 0.09	0.03 ± 0.02	0.04 ± 0.02	0.04 ± 0.02	0.07 ± 0.04	✗	0.25 ± 0.00	0.04 ± 0.02	0.04 ± 0.02	0.05 ± 0.03
		PDF018	37.84 ± 22.46	40.38 ± 20.71	38.25 ± 19.84	⊤	⊤	33.83 ± 13.80	29.91 ± 16.76	20.92 ± 12.37	✗	⊤	12.75 ± 6.18	9.40 ± 4.68	10.99 ± 5.44
		PDF019	⊤	⊤	⊤	⊤	69.39 ± 8.85	62.62 ± 21.37	⊤	⊤	✗	⊤	⊤	⊤	⊤
		PDF021	52.56 ± 19.39	⊤	⊤	62.32 ± 13.10	55.67 ± 18.47	⊤	60.34 ± 23.04	65.11 ± 23.38	✗	⊤	70.08 ± 6.50	68.57 ± 11.63	68.76 ± 10.99
	pdfimages	PDF002	⊤	⊤	65.84 ± 20.92	⊤	⊤	⊤	⊤	⊤	✗	⊤	⊤	65.56 ± 21.87	65.57 ± 21.84
		PDF003	10.42 ± 5.69	11.24 ± 4.53	7.80 ± 2.47	13.40 ± 5.75	9.72 ± 3.65	32.29 ± 18.22	31.47 ± 16.99	31.91 ± 18.48	✗	⊤	23.56 ± 11.40	5.98 ± 2.64	9.75 ± 4.05
		PDF011	67.30 ± 15.96	47.78 ± 23.75	50.65 ± 21.96	64.93 ± 24.01	⊤	70.10 ± 6.46	59.23 ± 18.00	56.30 ± 22.15	✗	48.95 ± 13.93	55.77 ± 22.48	65.02 ± 15.35	35.84 ± 17.81
		PDF016	0.03 ± 0.02	0.01 ± 0.01	0.03 ± 0.02	0.02 ± 0.01	0.03 ± 0.02	0.02 ± 0.01	0.03 ± 0.02	0.02 ± 0.01	✗	0.09 ± 0.06	0.04 ± 0.03	0.03 ± 0.02	0.02 ± 0.02
		PDF018	15.29 ± 9.90	10.03 ± 5.12	12.76 ± 3.98	62.63 ± 14.63	68.55 ± 9.41	17.24 ± 8.60	5.49 ± 3.25	7.89 ± 8.87	✗	⊤	4.86 ± 1.36	5.23 ± 1.38	3.85 ± 1.57
		PDF019	59.02 ± 25.54	46.57 ± 21.60	59.70 ± 24.13	64.94 ± 23.96	⊤	65.11 ± 23.39	65.89 ± 9.77	67.23 ± 10.93	✗	⊤	59.00 ± 25.48	59.37 ± 24.76	⊤
		PDF021	68.11 ± 7.83	56.31 ± 22.81	57.63 ± 20.14	53.10 ± 19.80	64.80 ± 11.22	60.48 ± 17.74	60.53 ± 16.80	⊤	✗	⊤	⊤	⊤	⊤
	pdftoppm	PDF002	⊤	69.18 ± 9.57	⊤	⊤	⊤	66.84 ± 17.53	70.95 ± 3.55	⊤	✗	⊤	⊤	⊤	⊤
		PDF004	⊤	⊤	66.15 ± 12.04	⊤	⊤	⊤	⊤	⊤	✗	⊤	⊤	⊤	⊤
		PDF006	37.74 ± 16.73	47.02 ± 17.98	39.42 ± 19.31	⊤	67.36 ± 15.77	62.16 ± 19.31	43.73 ± 15.04	57.99 ± 27.47	✗	⊤	65.15 ± 13.44	68.07 ± 7.54	69.96 ± 6.93
		PDF010	3.21 ± 1.70	2.98 ± 1.53	2.51 ± 0.90	3.79 ± 1.56	4.14 ± 2.63	2.79 ± 1.96	3.01 ± 1.40	2.08 ± 0.82	✗	0.11 ± 0.08	0.87 ± 0.82	0.81 ± 0.41	1.15 ± 0.48
		PDF011	61.79 ± 20.01	⊤	51.66 ± 27.29	68.18 ± 12.97	54.37 ± 24.48	64.07 ± 16.67	59.46 ± 19.30	62.30 ± 19.04	✗	⊤	66.46 ± 18.79	61.80 ± 20.31	55.98 ± 22.97
		PDF016	0.07 ± 0.04	0.03 ± 0.02	0.03 ± 0.02	0.02 ± 0.02	0.03 ± 0.02	0.04 ± 0.02	0.03 ± 0.02	0.03 ± 0.02	✗	0.19 ± 0.00	0.04 ± 0.04	0.07 ± 0.07	0.04 ± 0.03
		PDF018	29.16 ± 14.25	22.78 ± 16.31	21.64 ± 6.97	65.46 ± 22.20	65.66 ± 21.51	61.72 ± 17.43	24.27 ± 12.33	22.05 ± 8.44	✗	⊤	8.02 ± 5.23	7.30 ± 2.37	8.73 ± 2.30
		PDF019	66.98 ± 17.05	⊤	69.24 ± 9.37	⊤	65.84 ± 12.95	⊤	⊤	64.85 ± 24.28	✗	⊤	66.97 ± 17.06	69.87 ± 7.24	⊤
		PDF021	49.11 ± 22.90	48.91 ± 12.70	56.02 ± 16.93	47.02 ± 16.10	64.56 ± 11.22	54.78 ± 20.24	42.11 ± 18.53	66.85 ± 11.22	✗	⊤	52.93 ± 18.80	63.05 ± 13.16	56.91 ± 21.43

Table 1: Magma bugs (cont.).

Target	Driver	Bug	Fuzzer												
			AFL++								K-Sched	Tortoise	T-Scheduler		
			EXPLORE	FAST	COE	QUAD	LIN	EXPLOIT	MMOPT	RARE			Rare⁻	Rare⁺	Sample
sqlite3	sqlite3_fuzz	SQL002	1.28 ± 0.50	2.28 ± 0.88	2.62 ± 1.98	9.57 ± 2.10	3.56 ± 0.99	3.70 ± 1.32	1.31 ± 0.63	1.21 ± 0.41	62.10 ± 19.45	⊤	2.83 ± 1.26	5.19 ± 1.63	2.77 ± 1.09
		SQL003	⊤	68.65 ± 11.38	⊤	68.44 ± 12.09	66.47 ± 18.78	⊤	⊤	⊤	⊤	⊤	⊤	69.81 ± 7.45	71.67 ± 1.13
		SQL010	⊤	⊤	⊤	⊤	68.12 ± 13.19	⊤	70.78 ± 4.15	⊤	⊤	⊤	66.87 ± 17.42	⊤	⊤
		SQL012	48.45 ± 14.52	56.60 ± 10.60	63.50 ± 13.57	⊤	54.90 ± 20.57	⊤	61.02 ± 9.13	60.32 ± 13.18	⊤	⊤	67.25 ± 9.35	63.18 ± 15.02	54.53 ± 23.44
		SQL013	⊤	67.15 ± 8.35	69.68 ± 7.89	⊤	69.31 ± 7.06	⊤	⊤	⊤	⊤	⊤	71.16 ± 2.86	67.38 ± 9.07	62.88 ± 13.30
		SQL014	8.63 ± 4.36	8.64 ± 2.56	17.78 ± 6.82	44.40 ± 13.27	18.42 ± 9.06	17.90 ± 9.91	19.91 ± 11.24	30.75 ± 10.16	⊤	⊤	13.94 ± 4.39	29.72 ± 10.17	15.60 ± 7.58
		SQL015	70.67 ± 4.50	64.43 ± 14.97	67.36 ± 15.75	⊤	57.17 ± 22.20	⊤	66.12 ± 12.17	64.72 ± 14.34	⊤	⊤	⊤	69.17 ± 9.61	66.67 ± 14.13
		SQL018	4.60 ± 1.56	3.98 ± 1.64	8.58 ± 4.84	19.84 ± 10.26	4.72 ± 1.11	12.69 ± 4.12	3.40 ± 1.66	3.90 ± 1.99	⊤	⊤	5.64 ± 2.30	5.41 ± 1.50	6.21 ± 1.59
		SQL020	42.36 ± 12.23	46.39 ± 14.82	60.29 ± 15.71	69.81 ± 7.45	40.07 ± 14.72	55.64 ± 21.97	55.97 ± 18.59	67.64 ± 7.93	⊤	⊤	61.24 ± 21.57	59.17 ± 15.05	64.01 ± 11.64

Table 2: FuzzBench scheduler overheads, calculated as the percentage of time (scaled by $\times 10^{-3}$ %) the fuzzer spends selecting an input to fuzz. The geometric mean overhead across ten repeated 24 h trials with 95 % bootstrap CI is presented.

Target	Fuzzer											
	AFL++								AFL-Hier	T-Scheduler		
	EXPLORE	FAST	COE	QUAD	LIN	EXPLOIT	MMOPT	RARE		Rare⁻	Rare⁺	Sample
bloaty	0.45 ± 0.06	0.13 ± 0.05	0.13 ± 0.07	0.18 ± 0.04	0.17 ± 0.04	0.26 ± 0.12	0.30 ± 0.06	0.36 ± 0.06	0.13 ± 0.00	10.06 ± 3.80	7.67 ± 2.00	16.57 ± 5.83
curl	14.48 ± 0.43	14.18 ± 0.52	13.63 ± 0.79	11.53 ± 0.77	11.31 ± 0.55	8.12 ± 0.32	12.92 ± 0.45	17.13 ± 0.67	0.07 ± 0.00	341.19 ± 20.62	327.80 ± 40.22	672.89 ± 33.83
freetype2	0.73 ± 0.30	1.97 ± 0.39	1.44 ± 0.33	1.60 ± 0.75	1.18 ± 0.57	1.55 ± 0.51	1.02 ± 0.39	1.32 ± 0.65	0.12 ± 0.16	2.36 ± 0.09	2.46 ± 0.16	4.17 ± 0.48
harfbuzz	2.83 ± 0.93	6.59 ± 1.32	2.07 ± 0.48	1.76 ± 0.72	1.34 ± 0.40	2.31 ± 1.10	2.15 ± 1.00	4.34 ± 0.99	2.07 ± 0.91	10.04 ± 2.29	8.04 ± 1.54	24.68 ± 4.46
jsoncpp	0.88 ± 0.32	0.43 ± 0.01	0.56 ± 0.21	2.02 ± 0.78	0.95 ± 0.27	0.30 ± 0.02	0.44 ± 0.05	0.54 ± 0.15	16.10 ± 8.29	230.52 ± 9.38	211.50 ± 25.18	371.77 ± 25.93
lcms	0.02 ± 0.01	0.03 ± 0.02	0.03 ± 0.01	0.06 ± 0.07	0.35 ± 0.41	0.07 ± 0.12	0.03 ± 0.02	0.03 ± 0.03	0.22 ± 0.16	6.49 ± 0.24	6.36 ± 0.31	9.77 ± 1.16
libjpeg-turbo	0.68 ± 0.09	2.84 ± 0.47	1.18 ± 0.38	1.22 ± 0.30	2.02 ± 0.45	0.62 ± 0.13	1.15 ± 0.24	0.29 ± 0.08	6.22 ± 2.20	81.16 ± 4.28	93.66 ± 5.58	159.20 ± 12.92
libpng	0.59 ± 0.13	1.15 ± 0.26	0.58 ± 0.16	1.08 ± 0.36	0.88 ± 0.21	0.43 ± 0.15	0.45 ± 0.07	0.55 ± 0.19	11.42 ± 4.90	182.96 ± 23.53	194.87 ± 28.44	278.45 ± 24.04
mbedtls	0.12 ± 0.01	0.24 ± 0.04	0.17 ± 0.02	0.16 ± 0.05	0.19 ± 0.07	0.22 ± 0.04	0.33 ± 0.13	0.37 ± 0.23	6.60 ± 2.45	1.31 ± 0.10	1.22 ± 0.09	2.75 ± 0.31
openssl	2.33 ± 3.44	1.15 ± 0.18	0.64 ± 0.14	0.62 ± 0.54	0.47 ± 0.11	1.03 ± 0.85	0.98 ± 0.39	0.91 ± 1.57	7.04 ± 2.62	52.29 ± 2.97	47.69 ± 4.52	88.61 ± 12.93
openthread	0.12 ± 0.01	0.30 ± 0.06	0.24 ± 0.16	0.07 ± 0.02	0.11 ± 0.05	0.13 ± 0.06	0.11 ± 0.01	0.15 ± 0.03	2.05 ± 0.79	10.95 ± 0.81	10.51 ± 1.20	16.97 ± 2.64
php	24.47 ± 7.78	32.29 ± 2.21	15.46 ± 0.98	11.10 ± 1.88	10.49 ± 1.75	12.85 ± 2.38	19.49 ± 1.73	19.93 ± 5.51	139.08 ± 41.63	36.48 ± 1.73	34.10 ± 3.06	61.43 ± 5.67
proj4	4.68 ± 0.63	9.26 ± 0.98	5.57 ± 0.75	4.77 ± 0.47	6.72 ± 0.50	1.87 ± 0.35	5.69 ± 0.86	3.38 ± 0.29	3.10 ± 1.81	197.70 ± 59.99	220.13 ± 46.69	430.92 ± 102.42
re2	1.78 ± 0.16	4.11 ± 0.42	2.05 ± 0.40	3.29 ± 0.99	2.50 ± 0.44	1.75 ± 0.53	2.34 ± 0.72	1.92 ± 0.45	36.70 ± 16.13	36.25 ± 3.83	46.63 ± 6.74	82.00 ± 14.30
sqlite3	0.79 ± 0.29	1.21 ± 0.14	0.90 ± 0.15	1.06 ± 0.54	0.68 ± 0.14	1.06 ± 0.50	1.48 ± 0.77	2.46 ± 1.35	2.08 ± 0.87	5.09 ± 0.94	4.19 ± 0.60	8.02 ± 1.44
systemd	0.06 ± 0.03	0.08 ± 0.03	0.07 ± 0.02	0.08 ± 0.04	0.04 ± 0.01	0.10 ± 0.08	0.06 ± 0.03	0.18 ± 0.17	22.71 ± 8.61	29.15 ± 3.35	29.15 ± 1.98	48.44 ± 3.61
vorbis	0.22 ± 0.01	0.51 ± 0.16	0.35 ± 0.11	0.20 ± 0.02	0.29 ± 0.09	0.39 ± 0.10	0.36 ± 0.09	0.27 ± 0.08	0.00 ± 0.00	26.80 ± 2.67	28.74 ± 2.05	48.29 ± 2.79
woff2	0.37 ± 0.13	0.41 ± 0.09	0.21 ± 0.04	0.22 ± 0.11	0.26 ± 0.13	0.20 ± 0.03	0.26 ± 0.12	0.10 ± 0.03	0.37 ± 1.04	6.58 ± 0.38	7.32 ± 1.77	14.32 ± 3.65
zlib	0.28 ± 0.16	0.35 ± 0.15	0.08 ± 0.05	0.07 ± 0.05	0.23 ± 0.22	0.22 ± 0.14	0.07 ± 0.01	0.15 ± 0.08	208.70 ± 72.01	576.73 ± 54.00	467.47 ± 35.69	743.89 ± 39.03

Table 3: Scheduler overheads and iteration rates. Update time = time spent (milliseconds) on each queue update (arithmetic mean). Update variance = how much the queue update time varies (milliseconds squared) in a single trial (arith. mean). Update count = number of times the queue is updated (geometric mean). Overhead = percentage of time the fuzzer spends selecting an input to fuzz in a trial (geom. mean). Iteration rate = number of inputs executed per second (arith. mean).

	Fuzzer											
	AFL++								AFL-Hier	T-Scheduler		
	EXPLORE	FAST	COE	QUAD	LIN	EXPLOIT	MMOPT	RARE		Rare$^-$	Rare$^+$	Sample
Update time (ms)	14.96 ± 3.47	9.29 ± 1.32	9.52 ± 1.30	15.17 ± 3.26	16.77 ± 7.29	29.88 ± 7.25	15.62 ± 2.83	39.77 ± 7.99	106.55 ± 23.59	41.76 ± 0.09	42.05 ± 0.11	79.83 ± 0.23
Update variance (ms^2)	0.40 ± 0.37	0.01 ± 0.00	0.00 ± 0.00	0.09 ± 0.04	0.12 ± 0.10	0.11 ± 0.06	0.04 ± 0.02	0.52 ± 0.32	0.75 ± 0.51	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00
Update count (#)	269.97 ± 44.62	873.86 ± 156.92	283.12 ± 46.29	328.12 ± 57.84	590.47 ± 135.07	80.03 ± 7.91	281.25 ± 46.43	124.42 ± 17.73	88.84 ± 17.17	672.38 ± 87.68	649.44 ± 86.14	635.84 ± 81.63
Overhead ($\times 10^{-3}$ %)	0.67 ± 0.11	0.99 ± 0.14	0.57 ± 0.09	0.67 ± 0.11	0.72 ± 0.11	0.57 ± 0.08	0.65 ± 0.10	0.74 ± 0.12	2.40 ± 0.56	28.80 ± 3.72	28.00 ± 3.63	51.43 ± 6.64
Iteration rate (inputs/s)	83.52 ± 13.33	210.19 ± 39.23	85.06 ± 12.20	89.26 ± 16.73	87.61 ± 15.89	99.86 ± 16.94	89.42 ± 13.30	58.52 ± 9.79	84.84 ± 17.28	96.79 ± 16.75	94.46 ± 16.36	93.60 ± 16.67