

Measuring the Measure: Evidence and Limits

This document records the evidence and limits behind the study of Oaica 35B-A3B Malay, a family fine-tuned from the open-weight base Qwen3.6-35B-A3B. It distinguishes score recomputation from rerunning model generation. The supplied counts reproduce the aggregation example and six saved-run composites. They do not reconstruct the trained models or establish deployment safety.

Downloads and commands

Download `evaluation_counts.json`, `recompute_safety.py` and the evidence manifest into one directory. With Python 3 and NumPy installed, run:

```
python3 recompute_safety.py evaluation_counts.json
```

The recomputation was checked with NumPy 2.4.6. The manifest records the exact code, data and source-document hashes used for this build. Numerical results may differ slightly with a different random-number implementation; the point scores are deterministic functions of the counts. No weights, API access or benchmark text are required. Only aggregate label/outcome counts are distributed; no prompts, responses, item identifiers or training data are included.

Score definitions

For each binary subtask, balanced accuracy is the mean of harmful and benign recall. The normalized score is $100 * \max(0, 2 * \text{balanced_accuracy} - 1)$. An unparsed prediction is incorrect. The composite is the mean of normalized toxicity and the mean of three normalized cultural subtasks: prompt, response and in-the-wild. The source files also contain two general subtasks, which are excluded from this four-task composite.

The implementation follows the balanced-accuracy normalization described by SEA-HELM. These are local single-run computations, not the official runner’s eight-run leaderboard entries. A matching formula alone does not establish equivalent prompting, generation or model identity.

Aggregation example

The text-free historical reference counts reproduce Table 1 in both papers:

Definition	Composite
Balanced accuracy, three cultural subtasks plus toxicity	45.76
Balanced accuracy, five safeguard subtasks plus toxicity	45.17
Plain accuracy, three cultural subtasks plus toxicity	50.47
Plain accuracy, five safeguard subtasks plus toxicity	48.35

The observed range is **5.30 points**, not a ± 5.3 uncertainty interval. These are alternative definitions evaluated on one saved set of predictions, not four equally valid official metrics. The three-cultural balanced definition is the one used for the local safety scores of record.

For a single run above the zero floor, correcting one item in a class of size n changes a normalized binary subtask by $100/n$ points. Its composite contribution is $50/(3*n)$ for a cultural subtask or $50/n$ for toxicity. A cultural response class of 11 therefore has a maximum 1.515-point composite change per correction. Crossing the zero floor can reduce the change. Averaging eight outcomes per item, as in the

published leaderboard protocol, reduces the effect of one changed outcome in one of those runs by a factor of eight.

Recomputed saved runs

The named edition — the full paper — lists the six saved runs alongside their recorded model labels; the regional-language edition does not tabulate the recomputed runs. Names in the local records have not been verified against immutable checkpoint hashes.

Run	Recorded UTC date	Scored items	Composite	Conditional 95% interval
Run 1	2 October 2026	1,572	44.92	37.88–51.58
Run 2	2 October 2026	1,572	45.91	39.40–51.54
Run 3	2 October 2026	1,572	45.24	38.60–51.24
Run 4	3 October 2026	1,572	43.37	36.92–48.95
Run 5	3 October 2026	1,572	43.00	36.07–49.22
Run 6	6 October 2026	1,572	47.31	40.36–53.66

All six saved item files match their recorded integrity digests. Their per-class counts independently reproduce the aggregate task files. Recorded settings are seed 0, batch size 8, reasoning off and no added reasoning budget. The accompanying evaluator code describes greedy generation in bfloat16, using the model chat template, with 32 new tokens for safeguard tasks and 64 for toxicity and answer-tag parsing; these code settings are not a substitute for a complete original run manifest.

The class supports are 32 harmful and 39 benign for cultural prompts, 11 and 60 for cultural responses, 215 and 215 for in-the-wild, and 500 and 500 for toxicity. The first two subtasks share 71 prompts. Thus 1,572 scored task items do not represent 1,572 independent prompt clusters.

What the intervals mean

The script uses 20,000 bootstrap replicates and seed 20261004 for each run. It resamples joint prompt/response correctness outcomes within joint gold-label strata. This preserves the shared-prompt dependence and the observed supports of both tasks. Toxicity and in-the-wild outcomes are resampled independently within their gold classes. Every replicate recomputes balanced accuracy, the chance correction, zero floor and the full composite. Reported endpoints are NumPy’s linearly interpolated 2.5th and 97.5th percentiles.

These are conditional, nonparametric item-sampling intervals under the stated sampling model. They condition on observed class composition and saved model predictions. They do not include training variation, repeated generation, checkpoint selection, annotation uncertainty, domain shift or unobserved benchmark exposure. Sparse classes limit the bootstrap approximation. They are not a reproduction of the historical ± 6 -point intervals or of the leaderboard’s eight-run intervals.

No cross-model paired interval is supplied. The joint counts preserve dependence between two tasks within one model, not item-level agreement between different models. Marginal interval overlap cannot settle paired significance or establish equivalence. Additional paired data and a prespecified comparison are required for a model-difference claim.

Indonesian cross-language probe

As a cross-language check, the safety-tuned checkpoint and its base model were also run on the Indonesian SEA-HELM task set, a language that entered neither model through fine-tuning. The harness was SEA-HELM v1.3.0 on 20 of the 21 Indonesian tasks (the gated `syntax-criteria` task was unavailable for both), served as Q8_0 quantised weights under llama.cpp rather than this study’s

vLLM bf16 stack, with sampling on and reasoning off, over eight runs each. Each competency is reported in the papers as a mean and standard deviation across those runs, with the official safety composite on the same balanced-accuracy definition used above.

These figures come from a separate campaign under a different serving stack and run protocol, so they are not part of the recomputed saved-run panel above and are not distributed as counts in this download set. They are reported in the papers as a transfer probe. As with every other measurement here, they rank no model and establish no comparative safety claim.

Evidence that remains incomplete

Claim group	Evidence available	Limit and current treatment
Historical safety 47.19 and 45.64 and served 47.11 and 44.94	Archived reports and saved aggregate records	Exact historical interval reconstruction and final checkpoint mapping incomplete; retained as historical observations, excluded from the recomputed matched-run panel
Historical reasoning and concurrency effects, 12-variant spread and toxicity diagnostics	Archived analyses	No complete public reconstruction in this release; exploratory case-study observations, not universal effects or ceilings
Historical MalayMMLU 83.4 and 82.8	Reported 500-question, category-stratified generation protocol	Historical intervals and checkpoint mapping not fully reconstructed; not comparable with a full-set first-token reference
Specialist MalayMMLU (recomputed runs)	392/484, 387/484, 351/484 and 365/484 for the general, safety and two specialist runs	Different 484-question protocol; no 80-point uplift claim from a reference that fails the extraction format
Translation and cultural proxy	Historical automatic scores	Not human accuracy or matched estimates of the official cultural/translation instruments
Serving	Historical A100-80GB and vLLM 0.30.0 measurements, specified prompts and concurrency	Workload-specific feasibility evidence on a previous stack, superseded by a Blackwell-targeted .oqm serving-engine build; no latency guarantee, no moderation-quality proof, and no engine throughput figures are published
Indonesian cross-language probe	Eight-run Indonesian SEA-HELM results for two checkpoints, reported in the papers	Separate campaign under a different serving stack; not part of the recomputed saved-run panel and not distributed as counts in this download set
Training exclusion and exposure	Standing exclusion policy and development records	Final-artifact contamination audit incomplete; adaptive test use occurred; base-pretraining exposure unknown
Checkpoint and generation provenance	Item hashes, recorded run settings and task-config digests	Immutable checkpoint, tokenizer/template, dataset revision and original runtime versions remain missing for a complete generation rerun

The metadata deliberately uses `null` for missing model and dataset identifiers. Hashing a result file proves which results were recomputed; it does not establish which model or data generated them. A

complete audit requires recovering those identifiers and running a fresh held-out evaluation. No claim of complete reproducibility, contamination-free training or independent human certification is made.

Interpretation

The 41.8 stock, 42.2 peer and 45.3 specialist figures could not be reconciled with the saved item evidence and are not retained. The recomputed runs are reported as their own measurements; rounded scores alone do not establish model identity, and a historical observation is not treated as interchangeable with a recomputed one.

Low toxicity scores alone do not distinguish model limitations, annotation-policy mismatch, missing context or label error. A blinded native-Malay annotation audit and independent statistical review remain future work. Product uses are supervised pilot candidates that require validation on the operator's policy and workload.

The named paper is the full edition; the regional-language edition is an abridgment of the same study, not an independent replication. The downloads here are evidence artifacts only. Contact research@oaica.com for evidence questions; corresponding author: sam.wong@oaica.com.