Foundation-layer formalization design: finite fields, distributions, and a zero family

August 24, 2026

1 The setting

The low individual degree test of [JNV+20] works over a finite field $\mathbb{F}_q$, where $q = p^t$ is a prime power. The field structure enters the argument in two essential ways: through the polynomial calculus that supports the Schwartz–Zippel lemma, and through the additive characters $\omega^{\mathrm{tr}[\,\cdot\,]}$ used in the Fourier-analytic estimates. In addition, the proofs make constant use of expectations over uniform distributions on $\mathbb{F}_q^m$, on lines, and on sampled question pairs. These three ingredients— the field, the distributions, and the conventions used to manipulate them—constitute what we shall call the *foundation layer* of the formalization.[1]

In adapting the paper to a formal proof assistant we are obliged to make explicit several conventions that the prose leaves implicit: how to record the prime-power hypothesis on q, how to represent finitely supported probability distributions, and what to do with operator families that the paper never names but which arise as algebraic zero objects in the formal manipulations. We record those conventions here and verify that none of them silently change a hypothesis or conclusion of the cited argument.

2 The field parameter q

We are given that $q = p^t$ is a prime power; this is stated at the beginning of the preliminaries[2] of [JNV+20]. In the formal development we separate two roles played by this hypothesis. The *assertion* that q is a prime power is recorded as a bare existential

$$\exists\, p, n, \quad p \text{ prime},\ n \geq 1,\ q = p^n,$$

attached to a numerical value $q \in \mathbb{N}$ in a parameter record.[3] The *use* of a finite field of order q is delegated to a separate typeclass which bundles a field K, a

[1] The choices discussed here were collected in GitHub issue #458.

[2] See the source preamble in `references/ldt-paper/preliminaries.tex`, lines 17–19 and 89–93.

[3] The carrier and the prime-power witness live in the structure Parameters (`MIPStarRE/LDT/Basic/ParametersBase.lean`, line 36), with field hqPrimePower of the displayed existential type.

Fintype instance, and a coding bijection $K \simeq \mathsf{Fin}\, q$.[4]

Arithmetic on scalars is therefore carried out inside the field K, while combinatorial sums, expectations, and indexing pass through $\mathsf{Fin}\, q$ via the explicit decoding/encoding maps. The prime-power assertion is needed only to derive $q \geq 2$, the non-vanishing of $|\mathbb{F}_q|$, and the existence of an honest field of order q; these are exactly the properties used in the paper. The field $\mathbb{F}_q$ of the cited argument and the field inhabited by the typeclass are the same object up to canonical isomorphism. This is a matter of formalization design and not of mathematics: no hypothesis or conclusion is altered.

3 Probability distributions

The paper writes its averages in the standard informal style: the expectation $\mathbf{E}_{\boldsymbol{x} \in \mathbb{F}_q^m}$ over a uniform point, the expectation over a uniformly random line, and so on. In the formal development we make these explicit by representing a distribution as a finite support together with a non-negative real weight on each point, subject to an IsProbability predicate that the total weight equals 1.[5] The uniform distribution on a nonempty finite type is then a derived case, and every expectation in the paper becomes a finite sum over an explicit support.

This is a self-contained reimplementation of a fragment of measure theory, and is in principle redundant with the probability layer of Mathlib; we adopt the lighter-weight type because every distribution we encounter is finite and explicitly supported. It faithfully represents each of the paper's expectations, and no mathematical statement depends on the choice.

4 The zero family

The full-slice commutation transport requires a neutral element in the family of operator-valued measurements ordered by the state-dependent distance relation. We introduce for this purpose a measurement family in which every outcome and the total are equal to the zero operator.[6] Its safety is recorded by a single lemma[7] which bounds the state-dependent distance between this zero family and the actual full-slice product by 1 on a normalized state, an estimate that follows directly from the definitions.

The cited argument never names such a family. It instead writes out the corresponding inequalities directly, term by term. The zero family is therefore a packaging convenience for those same inequalities; it asserts nothing that the paper would contradict.

[4] This is the typeclass FieldModel params.q in `ParametersBase.lean`, line 224; its canonical instance is constructed from the prime-power witness via PrimePowerFieldSpec.toFieldModel, which produces the Mathlib finite field $\mathsf{GaloisField}\, p\, n$.

[5] The type Distribution is defined in `MIPStarRE/LDT/Basic/Distribution.lean` at line 17, with avgOver the corresponding average over the explicit support.

[6] The declaration zeroFullSliceOpFamily appears in `MIPStarRE/LDT/Commutativity/Transport/FullSlice.lean`, line 26.

[7] The lemma fullSliceProductLeft_to_zero_le_one in the same file, line 216.

5 Conclusion

There is no mathematical discrepancy. The formalization records the prime-power hypothesis on q as an existential proof and accesses the corresponding finite field through a typeclass; it represents the paper's expectations as finite weighted sums; and it introduces a zero measurement family purely as a packaging device for elementary inequalities already present in the paper. Each choice is a formalization decision, and each preserves the mathematics of the cited argument exactly.

References

[JNV$^+$20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Quantum soundness of the classical low individual degree test, 2020. arXiv:2009.12982.