The prime field is not a maximal clique in GP(5^8, 3): a Lean-certified counterexample to Yip's maximal subfield clique conjecture

DRAFT research manuscript, 1 November 2026. No human authorship or affiliation is asserted. Prepared with AI assistance (Claude Opus 5.5) within a user-directed research campaign. Zero accepted campaign credit; final replay, paper review and acceptance are reserved to the campaign root.

Abstract. For $d > 1$ and a prime power $q \equiv 1 \pmod{2d}$ of the prime p, Yip conjectured that the largest subfield $\mathbb{F}_{p^r}$ with $d \mid (q-1)/(p^r-1)$ is a maximal clique of the generalized Paley graph GP(q,d), whose edges join elements of $\mathbb{F}_q$ differing by a nonzero d-th power. We show that this fails for $q = 5^8$ and $d = 3$. Here the largest admissible r is 1, and in every field with 5^8 elements the prime field $\mathbb{F}_5$ is a clique that extends to the strictly larger clique $\mathbb{F}_5 \cup \{x\}$, where $x = 2\theta + 4\theta^2 + \theta^3$ and θ is any root of $X^8 + X^7 + 2X^6 + 2$. The proof uses a Frobenius chain certificate and ten explicit cube and inverse certificates; every step can be checked by hand or with a short computation. The negation of the conjecture, stated with literal definitions, is proved in Lean 4 with Mathlib using only the standard axioms. We also give ordinary proofs, outside the formal endpoint, that $\mathbb{F}_5 \oplus x\mathbb{F}_5$ is a 25-clique and that $\mathbb{F}_5$ is a maximal subfield clique. The latter shows that the hypothesis $q > (n-1)^2$ of Yip's 2023 theorem cannot simply be dropped, contrary to a conjecture stated there. That theorem itself remains valid.

mathdb:2611.00006v1 03 Nov 2026

1. Introduction

Let p be an odd prime, q a power of p, $d > 1$ and $q \equiv 1 \pmod{2d}$. The *d-Paley graph* GP(q,d) has vertex set $\mathbb{F}_q$; distinct g, h are adjacent iff $g - h \in (\mathbb{F}_q^*)^d$, the set of nonzero d-th powers. The congruence makes -1 a d-th power, so the graph is undirected. If $d \mid (q-1)/(p^k-1)$, every nonzero element of the subfield $\mathbb{F}_{p^k}$ is a d-th power, so $\mathbb{F}_{p^k}$ is a clique. This observation of Broere, Döman and Ridley is quoted in [1, Theorem 1.3]. Yip conjectured that the largest such subfield is always maximal [1, Conjecture 1.4]:

> *Conjecture (Yip). Let $d > 1$ be an integer. Let $q \equiv 1 \pmod{2d}$ be a power of a prime p, and let r be the largest integer such that $d \mid (q-1)/(p^r-1)$. Then the subfield $\mathbb{F}_{p^r}$ forms a maximal clique in GP(q,d).*

The same statement is Conjecture 1.1 of [2], and it is MathDB problem 355956 [6]. In [2], Theorem 1.2 proves the following. If $q^n \equiv 1 \pmod{2d}$, $q > (n-1)^2$, and $\mathbb{F}_q$ is a maximal subfield clique of GP(q^n,d), then $\mathbb{F}_q$ is a maximal clique. Note that in Theorem 1.2, q denotes the size of the base field. The abstract of [2] says that this "confirms a conjecture of Yip", and a remark after the proof adds: "We conjecture that the condition $q>(n-1)^2$ in Theorem 1.2 can be dropped." The same remark reports SageMath verification for $n \le 5$ (all $q \le (n-1)^2$) and for $n = 6$ with $q \le 17$. A later paper [3, §1] restates [2] without the size hypothesis: "if a generalized Paley graph GP(q,d) admits a clique which is a subfield of $\mathbb{F}_q$ and K is the largest such subfield, the author [Y23] used character sum estimates to show that K is a maximal clique." It adds: "It is also tempting to conjecture that $\omega(\mathrm{GP}(q,d)) = |K|$."

Main result. The unrestricted conjecture is false.

> ***Theorem 1.*** *Let K be any field with $5^8 = 390625$ elements, and let $\theta \in K$ be a root of $f = X^8 + X^7 + 2X^6 + 2$ (such a root exists). Put $x = 2\theta + 4\theta^2 + \theta^3$. Then $\mathbb{F}_5 \subset K$ is a clique of GP(5^8,3), $x \notin \mathbb{F}_5$, and $\mathbb{F}_5 \cup \{x\}$ is a clique. In particular $\mathbb{F}_5$ is not a maximal clique.*

> ***Corollary 2.*** *Yip's conjecture is false at $(q, d) = (5^8, 3)$, where the largest admissible r is 1.*

Theorem 1 and Corollary 2 are certified in Lean (Section 5). Section 4 contains two further statements with ordinary proofs only: the 25-clique $\mathbb{F}_5 \oplus x\mathbb{F}_5$, and the fact that $\mathbb{F}_5$ is a maximal subfield clique. It also lists computational diagnostics. Theorem 1.2 of [2] is not contradicted, because there the base field has $5 \le (8-1)^2 = 49$ elements. What fails is the unrestricted conjecture. The remark-conjecture in [2] that the size hypothesis can be dropped fails as well.

2. Definitions and the exact statement

mathdb:2611.00006v1 03 Nov 2026

Throughout, K is a finite field with $q = p^m$ elements, and $(K^*)^d = \{y^d : y \in K, y \neq 0\}$. GP(q,d) is the graph on K in which $g \sim h$ iff $g - h \in (K^*)^d$. A *clique* is a set $C \subseteq K$ whose distinct elements are pairwise adjacent. A *maximal clique* is a clique C such that every clique $C' \supseteq C$ equals C. For $r \mid m$, the subfield $\mathbb{F}_{p^r}$ of K is $\{z \in K : z^{p^r} = z\}$. The quotient $(q-1)/(p^r-1)$ in the conjecture is meant as an integer. This forces $r \geq 1$ and $p^r - 1 \mid p^m - 1$, that is, $r \mid m$. So r is the largest element of

$$A(p, m, d) = \{\, r \geq 1 : (p^r-1) \mid (p^m-1) \text{ and } d \mid (p^m-1)/(p^r-1) \,\}.$$

With these definitions the conjecture reads: *for all $d > 1$, all primes p, all $m \geq 1$ and all fields K with $|K| = p^m$ and $p^m \equiv 1 \pmod{2d}$, if $r = \max A(p,m,d)$, then $\mathbb{F}_{p^r}$ is a maximal clique of GP(p^m,d).* All fields of order p^m are isomorphic and the property is isomorphism-invariant, so quantifying over every K is equivalent to the source's "$\mathbb{F}_q$". A refutation needs one admissible (d, p, m), and Theorem 1 holds for every K of order 5^8.

3. Proof of Theorem 1

3.1 The parameters.

$q - 1 = 390624 = 2^5 \cdot 3 \cdot 13 \cdot 313 = 6 \cdot 65104$, so $q \equiv 1 \pmod 6$. Since $p^r - 1 \mid p^m - 1$ iff $r \mid m$, the candidates are $r \in \{1, 2, 4, 8\}$. Their quotients are listed below, and only $r = 1$ is admissible. Hence the conjecture asserts that $\mathbb{F}_5$ is a maximal clique of GP(5^8,3).

r	1	2	4	8
$(q-1)/(5^r-1)$	$97656 = 3 \cdot 32552$	$16276 \equiv 1 \pmod 3$	$626 \equiv 2 \pmod 3$	1

3.2 Characteristic and the prime field.

The characteristic of K is a prime dividing $|K| = 5^8$, so it is 5. In characteristic 5, $z^5 - z = z(z-1)(z-2)(z-3)(z-4)$, so $\{z \in K : z^5 = z\} = \{0,1,2,3,4\} = \mathbb{F}_5$.

3.3 A root of f in K.

In $\mathbb{F}_5[X]/(f)$ let t be the class of X; since $X^8 \equiv 4X^7 + 3X^6 + 3$, classes are represented by polynomials of degree at most 7. Write B_i for the residue of X^{5i} mod f. In characteristic 5, $(\Sigma\, c_i t^i)^5 = \Sigma\, c_i t^{5i}$ for $c_i \in \mathbb{F}_5$. Hence, if $t^{5^k} = P_k(t)$ with $P_k = \Sigma\, c_i X^i$, then $P_{k+1} = \Sigma\, c_i B_i$: one multiplication by the 8×8 Frobenius matrix whose rows are the B_i. Coefficients are listed from X^0 to X^7.

i	$B_i = X^{5i} \bmod f$	k	P_k with $t^{5^k} = P_k(t)$
0	`1 0 0 0 0 0 0 0`	0	`0 1 0 0 0 0 0 0`
1	`0 0 0 0 0 1 0 0`	1	`0 0 0 0 0 1 0 0`
2	`2 2 3 0 0 0 2 3`	2	`2 3 0 3 2 4 4 4`
3	`4 1 0 2 4 2 1 1`	3	`4 3 4 3 0 1 2 0`
4	`4 2 0 0 3 4 0 4`	4	`1 0 3 4 3 2 1 0`
5	`2 3 0 3 2 4 4 4`	5	`4 0 2 4 1 0 1 1`
6	`0 3 3 0 2 2 3 3`	6	`4 1 2 3 0 4 0 1`
7	`1 3 3 0 4 0 4 4`	7	`4 2 4 3 4 3 2 4`
		8	`0 1 0 0 0 0 0 0`

Since $P_8 = X$, $t^{5^8} = t$, so f divides $X^{5^8} - X$ in $\mathbb{F}_5[X]$ and therefore in K[X]. In K[X], $X^{|K|} - X = \prod_{a \in K}(X - a)$. By unique factorisation, the monic polynomial f is a product of 8 distinct linear factors over K, so a root $\theta \in K$ exists. Irreducibility of f is not needed here. The formal proof performs the same eight steps over K, inside AdjoinRoot(f). Each step is an exact identity $P_k(T)^5 - P_{k+1}(T) = A_k(T)f(T) + 5B'_k(T)$ in $\mathbb{Z}[T]$, and these identities are checked by `linear_combination`.

3.4 Cube certificates; why −1 is a cube.

For each $a \in \mathbb{F}_5$, the Lean module contains polynomials y_a, h_a of degree at most 7 with $y_a^3 \equiv x - a$ and $(x - a)h_a \equiv 1$ modulo $(f, 5)$, where $x = 2X + 4X^2 + X^3$:

a	y_a ($X^0 \dots X^7$)	h_a ($X^0 \dots X^7$)
0	0 4 3 3 2 3 0 0	3 2 2 0 4 4 4 3
1	3 4 4 4 1 1 0 4	2 3 3 0 0 3 4 3
2	4 4 3 4 4 3 1 2	2 1 2 0 2 3 2 3
3	2 1 0 4 0 0 4 0	2 4 2 4 0 1 1 0
4	0 0 1 2 2 4 0 3	1 0 1 2 2 2 1 0

Evaluating at θ gives $x - a = y_a(\theta)^3$ and $(x - a)\cdot h_a(\theta) = 1$ in K. Hence $x - a \neq 0$, so $y_a(\theta) \neq 0$, and $x - a$ is a nonzero cube. Checking one certificate means one product of polynomials of degree at most 7, reduced mod f over $\mathbb{F}_5$. Moreover $a - x = (-y_a(\theta))^3$, because $-1 = (-1)^3$ is a cube. More generally, $q \equiv 1 \pmod{2d}$ gives $d \mid (q-1)/2$, so $-1 = g^{(q-1)/2}$ is a d-th power for any generator g of K^*. Finally, every $w \in \mathbb{F}_5^*$ has $w^4 = 1$, so $w = w^9 = (w^3)^3$ is a cube.

3.5 The extension; proofs of Theorem 1 and Corollary 2.

Differences of distinct elements of $\mathbb{F}_5$ are nonzero elements of $\mathbb{F}_5$, hence cubes, so $\mathbb{F}_5$ is a clique. By §3.4, $x \neq a$, and both $x - a$ and $a - x$ are nonzero cubes, for every $a \in \mathbb{F}_5$. Thus $\mathbb{F}_5 \cup \{x\}$ is a clique that strictly contains $\mathbb{F}_5$, which proves Theorem 1. For Corollary 2, take $(d, p, m) = (3, 5, 8)$. Then $d > 1$, 5 is prime, $5^8 \equiv 1 \pmod 6$, and $\max A(5,8,3) = 1$ by §3.1. The conjecture would make $\mathbb{F}_5$ a maximal clique, contradicting Theorem 1. ∎

3.6 Supplement: irreducibility via the Frobenius orbit.

This step is not used above and is not formalised. Since $f \mid X^{5^8} - X$, f is squarefree and each of its irreducible factors over $\mathbb{F}_5$ has degree dividing 8. If f were reducible, every factor would have degree 1, 2 or 4 and so would divide $X^{5^4} - X$. Because the factors are distinct, f would then divide $X^{625} - X$, forcing $P_4 = X$. The table shows $P_4 \neq X$, so f is irreducible. Thus $\mathbb{F}_5[X]/(f)$ is a concrete model of $\mathbb{F}_{5^8}$, in which the Frobenius orbit $\theta, \theta^5, \dots, \theta^{5^7}$ has exact length 8. Rabin's test gives the same answer: $\gcd(f, P_4 - X) = 1$.

4. Consequences beyond the formal endpoint

The two propositions below have complete ordinary proofs built from Theorem 1. They are **not** part of the Lean endpoint.

Proposition 3. *$V = \mathbb{F}_5 \oplus x\mathbb{F}_5$ is a clique of size 25 in $GP(5^8,3)$; hence $\omega(GP(5^8,3)) \geq 25$.*

Proof. Take distinct $u = a + bx$ and $v = a' + b'x$ in V. If $b = b'$, then $u - v = a - a' \in \mathbb{F}_5^*$, which is a cube. If $b \neq b'$, then $u - v = (b - b')(x - c)$ with $c = (a' - a)/(b - b') \in \mathbb{F}_5$. This is a product of two nonzero cubes, hence a nonzero cube. Finally $|V| = 25$, because $x \notin \mathbb{F}_5$. ∎ This is the two-dimensional clique predicted by Yip's lemma [1, §2].

Proposition 4. *$\mathbb{F}_5$ is a maximal subfield clique of $GP(5^8,3)$: none of $\mathbb{F}_{25}$, $\mathbb{F}_{625}$, $\mathbb{F}_{5^8}$ is a clique.*

Proof. Let L be a subfield of K. The differences of distinct elements of L are exactly the elements of L^*, so L is a clique iff $L^* \subseteq (K^*)^3$. Now K^* is cyclic of order $q - 1$, and L^* is its unique subgroup of order $|L| - 1$. The cubes form the unique subgroup of index 3, of order $(q - 1)/3$. So $L^* \subseteq (K^*)^3$ iff $|L| - 1$ divides $(q - 1)/3$, that is, iff $3 \mid (q - 1)/(|L| - 1)$. For $|L| = 25$, 625 and 5^8, the quotients 16276, 626 and 1 are not divisible by 3. ∎ So the largest subfield clique has 5 elements, and Proposition 3 shows that the guess $\omega(GP(q,d)) = |K|$ mentioned in [3, §1] (where K denotes the largest subfield clique) fails here: $\omega(GP(5^8,3)) \geq 25 > 5$.

Apply [2, Theorem 1.2] with base field $\mathbb{F}_5$, $n = 8$ and $d = 3$. Then $5^8 \equiv 1 \pmod 6$, and $\mathbb{F}_5$ is a maximal subfield clique by Proposition 4, yet $\mathbb{F}_5$ is not a maximal clique by Theorem 1. The theorem is consistent with this, because its hypothesis

mathdb:2611.00006v1 03 Nov 2026

$5 > (8-1)^2$ fails. The remark in [2] that the condition $q > (n-1)^2$ "can be dropped" is therefore false. The case lies outside the computer checks reported in [2] ($n \le 5$; $n = 6$ with $q \le 17$). It is also outside the special case of [4] (n an odd prime, $q > n^2$) and the regime $q > (d-1)^2$ for GP(q^d,d) quoted in [5].

Computational diagnostics (corroboration only; never premises). An exhaustive discrete-log count over K, in this dossier's standard-library script, finds exactly 960 elements $y \notin \mathbb{F}_5$ with $\mathbb{F}_5 \cup \{y\}$ a clique; x is one of them. An independent review script found the same count. None of the 960 lies in $\mathbb{F}_{625}$, consistent with Yip's verification for $n \le 5$, which covers GP(625,3). The script also confirms that θ is a primitive element and that generators of $\mathbb{F}_{25}^*$ and $\mathbb{F}_{625}^*$ are non-cubes. Finally, the lane that found the counterexample searched every admissible case with $q \le 5 \cdot 10^6$ outside the range of [2, Theorem 1.2] (26 fields, 219 cases) and found only this failure. That search was not re-run here, and none of these counts is a Lean result.

5. Formal verification

The module `Yip355956.lean` (22,623 bytes, sha256 `0ccf6655…ee9d7be`) is copied byte-for-byte from the authoring lane. It imports only Mathlib, uses Lean 4.34.1 (commit `5045d005`), and Mathlib `d13f23b7`. Its literal statement of the conjecture is:

```
def YipConjecture : Prop :=
  ∀ (d p m : ℕ) (K : Type) [Field K] [Finite K], 1 < d → p.Prime → 0 < m →
    Nat.card K = p ^ m → p ^ m ≡ 1 [MOD 2 * d] →
    ∀ r : ℕ, IsGreatest (admissibleR p m d) r → IsMaximalGPClique K d (subfieldSet K (p ^ r))
theorem yip_conjecture_false : ¬ YipConjecture
```

`YipConjectureSG` is identical, except that its conclusion is `Maximal (fun s => (GPGraph K d).IsClique s) (subfieldSet K (p ^ r))` with `GPGraph K d := SimpleGraph.fromRel (GPAdj K d)`. It is refuted by `yip_conjecture_SG_false`. Both endpoints instantiate `GaloisField 5 8`, whose cardinality is proved, so the refutation is not vacuous. The table below lists every definition and every key lemma.

Lean name	Formal content (abridged)	Mathematical role
`dPowers K d`	{w | ∃ y, y ≠ 0 ∧ y^d = w}	$(K^*)^d$, connection set
`GPAdj K d g h`	g − h ∈ dPowers K d	adjacency in Cay(K^+, $(K^*)^d$)
`IsGPClique K d C`	∀ u v ∈ C, u ≠ v → GPAdj u v	clique
`IsMaximalGPClique`	clique ∧ ∀ C′ clique, C ⊆ C′ → C′ = C	maximal clique
`subfieldSet K pr`	{z | z^pr = z}	$\mathbb{F}_p{}^r$ inside K (r | m)
`admissibleR p m d`	{r | 0 < r ∧ p^r−1 | p^m−1 ∧ d | (p^m−1)/(p^r−1)}	A(p,m,d); r = its greatest element
`YipConjecture`	displayed above	the conjecture, all quantifiers
`admissibleR_greatest`	IsGreatest (admissibleR 5 8 3) 1	§3.1: r = 1
`five_eq_zero_of_card`, `mem_subfieldSet_iff`	|K| = 5^8 → 5 = 0; z^5 = z ↔ z ∈ {0,…,4}	§3.2
`fK_dvd`	(5 : K) = 0 → f | X^(5^8) − X in K[X]	§3.3 Frobenius chain
`exists_root`	|K| = 5^8 → ∃ θ, θ^8+θ^7+2θ^6+2 = 0	§3.3 splitting
`cube_a`, `inv_a` (a = 0…4)	y_a(θ)^3 = wit θ − a; (wit θ − a)·h_a(θ) = 1	§3.4 certificates
`wit_sub_mem`	x − a, a − x ∈ dPowers K 3 ∧ x ≠ a	§3.4, incl. −1 a cube
`small_sub_mem`	a ≠ b in {0,…,4} → a − b ∈ dPowers K 3	$\mathbb{F}_5$ is a clique
`not_maximal_of_card`	|K| = 5^8 → clique ∧ ¬ maximal	Theorem 1
`yip_conjecture_false`	¬ YipConjecture	Corollary 2
`not_maximal_SG_of_card`, `yip_conjecture_SG_false`	¬ Maximal (IsClique) …; ¬ YipConjectureSG	Mathlib SimpleGraph reading

mathdb:2611.00006v1 03 Nov 2026

mathdb:2611.00006v1 03 Nov 2026

Replay and audit. The dossier's portable driver takes the toolchain locations from LEAN_BIN and LEAN_PACKAGES. Before running anything it checks the pinned binary hashes and the source manifest, and it refuses to start if any `.olean` already exists. It then performs these steps:

(i) a strict build: `lean -j1 -DwarningAsError=true`;

(ii) a kernel re-check with `leanchecker`;

(iii) a reviewer audit of all 40 constants stored in the module's data, including auxiliary and generated ones. For each constant it prints the full type with `pp.all`, checks body presence via `value? true`, checks safe and non-partial status and the absence of new axioms, and requires transitive axioms within {propext, Classical.choice, Quot.sound};

(iv) sanity re-statements of the endpoints;

(v) negative controls: a wrong certificate ($x - 1$ in place of $x - 0$) is rejected by `linear_combination`, while its verbatim twin is accepted; the endpoint does not typecheck as the conjecture itself; `sorry` is rejected in strict mode; the axiom filter flags an added axiom; and a malformed `.olean` fails `leanchecker` with an invalid-header error. Each control asserts only what it tests.

No `sorry`, `admit`, new axiom, `unsafe`, `native_decide` or `ofReduceBool` occurs. The only finite case analysis is an `interval_cases`/`decide` check on $r \le 8$, which is kernel-checked.

Certified in Lean	Ordinary proof only	Computation only (diagnostic)
$r = 1$; $\mathbb{F}_5$ is a clique; f has a root in every K with $\lvert K\rvert = 5^8$; $x - a$ and $a - x$ nonzero cubes; $\mathbb{F}_5$ not maximal; ¬YipConjecture and ¬YipConjectureSG	irreducibility of f (§3.6); 25-clique and $\omega \ge 25$ (Prop. 3); $\mathbb{F}_5$ a maximal subfield clique (Prop. 4); failure of the remark-conjecture of [2]	960 extension vertices, none in the subfield of order 625; θ primitive; author sweep up to $5 \cdot 10^6$ (only failure)

6. Trust, scope and novelty limits

Formal trust. The Lean kernel, the Lean compiler and the prebuilt Mathlib dependency `.olean` files are trusted. The upstream dependencies were not rebuilt from source here, and `leanchecker` comes from the same installation, so the kernel check is not independent of the toolchain. Faithfulness of `YipConjecture` to the source statement is a matter of human reading. Section 2 records the interpretation used: $r \ge 1$ and integral quotients. An independent technical review reached the same reading, and our own reading of [1, 2] agrees with it.

Resource note. Each tool call ran on at most 2 CPUs, with CPU time ≤ 120 s, wall time ≤ 140 s, an address space of 64 GiB and MALLOC_ARENA_MAX=2. Where available, each call also ran inside a systemd scope with MemoryMax=6G. The 6 GiB sampled-RSS guard applies to private memory (anonymous plus shmem). Importing Mathlib maps about 6–7 GB of read-only `.olean` files, so total VmRSS, which counts those clean file-backed pages, exceeded 6 GiB. The receipts report both quantities.

Scope. We refute the unrestricted conjecture and the remark-conjecture of [2]. We make no claim about which pairs (q, d) fail in general, about the exact clique number of $GP(5^8,3)$, or about a corrected sharp hypothesis. [2, Theorem 1.2] remains valid. The abstract of [2] says "confirms", and [3, §1] restates [2] without the size hypothesis; both should be read with that hypothesis in mind.

Novelty. We make no claim of worldwide priority. The search for prior art was bounded. It read the bodies of [1]–[5]. Among works citing [1], three listed by OpenAlex were not read, and neither was Yip's doctoral thesis. Web and registry searches on 1 November 2026 found no report of this counterexample. The MathDB/Palomar comment and solution state could not be accessed (HTTP 403). MathDB lists the problem as open, but its references field attaches a quotation about the Peisert-graph analogue that is unrelated to this conjecture.

AI assistance. The counterexample and the Lean module were produced in an earlier AI-assisted research lane of the same campaign. Separate AI-assisted lanes then reviewed its technical fidelity and its novelty and significance. This manuscript and its dossier were prepared with AI assistance (Claude Opus 5.5). No human has reviewed this draft.

References

[1] C. H. Yip, On maximal cliques of Cayley graphs over fields, J. Algebraic Combin. 56(2) (2022) 323–333; arXiv:2101.09652 (v2 TeX source read). Conjecture 1.4; Theorem 1.3 (Broere–Döman–Ridley); lemma in §2.

[2] C. H. Yip, Maximality of subfields as cliques in Cayley graphs over finite fields, Algebr. Comb. 6(4) (2023) 901–905, doi:10.5802/alco.291; arXiv:2209.00864 (published TeX and arXiv v2 TeX read). Conjecture 1.1, Theorem 1.2 and the remark after its proof.

[3] C. H. Yip, Exact values and improved bounds on the clique number of cyclotomic graphs, arXiv:2304.13213 (v5 TeX read; recorded by the independent source review as published in Des. Codes Cryptogr., 2025; journal version not read).

[4] S. Asgarli and C. H. Yip, Van Lint–MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields, J. Combin. Theory Ser. A 192 (2022) 105667; arXiv:2106.01522 (TeX read; restates the conjecture and proves the case n an odd prime, $q > n^2$).

[5] G. Martin and C. H. Yip, Distribution of power residues over shifted subfields and maximal cliques in generalized Paley graphs, arXiv:2403.04312 (TeX read; journal version not read).

[6] MathDB problem 355956, "Yip's maximal subfield clique conjecture for generalized Paley graphs", https://mathdb.com/p/355956/ (raw record from the 2026-09-29 corpus snapshot, sha256 4d6b71c7…6d81d; live page not accessed).

[7] The Lean 4 theorem prover, v4.34.1, commit 5045d0056413266e57c625dcd7c365b10e377c52; The Mathlib Community, Mathlib, commit d13f23b723b8a846827a245b89c10fc7d3f11612.

mathdb:2611.00006v1 03 Nov 2026