



# *ALGEBRAIC COMBINATORICS*


Chi Hoi Yip

**Maximality of subfields as cliques in Cayley graphs over finite fields**

Volume 6, issue 4 (2023), p. 901-905.

<https://doi.org/10.5802/alco.291>

© The author(s), 2023.

 This article is licensed under the  
CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE.  
<http://creativecommons.org/licenses/by/4.0/>



*Algebraic Combinatorics is published by The Combinatorics Consortium  
and is a member of the Centre Mersenne for Open Scientific Publishing*  
[www.tccpublishing.org](http://www.tccpublishing.org)    [www.centre-mersenne.org](http://www.centre-mersenne.org)  
e-ISSN: 2589-5486





# Maximality of subfields as cliques in Cayley graphs over finite fields

Chi Hoi Yip

**ABSTRACT** We show the maximality of subfields as cliques in a special family of Cayley graphs defined on the additive group of a finite field. In particular, this confirms a conjecture of Yip on generalized Paley graphs.

## 1. INTRODUCTION

Throughout the paper, let  $p$  be an odd prime and  $q$  a power of  $p$ . Let  $\mathbb{F}_q$  be the finite field with  $q$  elements,  $\mathbb{F}_q^+$  be its additive group, and  $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$  be its multiplicative group.

In this paper we study maximal cliques in Cayley graphs. We begin by recalling some basic terminologies. Given an abelian group  $G$  and a connection set  $S \subset G \setminus \{0\}$  with  $S = -S$ , the *Cayley graph*  $\text{Cay}(G, S)$  is the undirected graph whose vertices are elements of  $G$ , such that two vertices  $g$  and  $h$  are adjacent if and only if  $g - h \in S$ . A *clique* in a graph  $X$  is a subset of vertices in  $X$  such that every two distinct vertices in the clique are adjacent. The clique number of  $X$ , denoted by  $\omega(X)$ , is the size of a maximum clique in  $X$ . A *maximal clique* is a clique that is not contained in a strictly larger clique.

Generalized Paley graphs are well-studied Cayley graphs. They were first introduced by Cohen [4] in 1988, and have been reintroduced by several groups of authors. Let  $d > 1$  be a positive integer and  $q \equiv 1 \pmod{2d}$ . The  *$d$ -Paley graph* on  $\mathbb{F}_q$ , denoted  $GP(q, d)$ , is the Cayley graph  $\text{Cay}(\mathbb{F}_q^+, (\mathbb{F}_q^*)^d)$ , where  $(\mathbb{F}_q^*)^d$  is the set of  $d$ -th powers in  $\mathbb{F}_q^*$ . Note that the condition  $q \equiv 1 \pmod{2d}$  avoids degeneracy of the graph; see for example [4, Section 4]. Note that Paley graphs are simply 2-Paley graphs. 3-Paley graphs and 4-Paley graphs are also known as *cubic Paley graphs* and *quadruple Paley graphs*.

It is known that in the Paley graph  $GP(q^2, 2)$ , the subfield  $\mathbb{F}_q$  forms a maximal clique for a trivial reason [3]: the clique number of  $GP(q^2, 2)$  is  $q$ . In general, Broere, Döman, and Ridley [3] observed that in the generalized Paley graph  $GP(q^n, d)$ , the subfield  $\mathbb{F}_q$  forms a clique if  $d \mid \frac{q^n - 1}{q - 1}$ . In this case, this observation leads to  $\omega(GP(q^n, d)) \geq q$ , which is much better than the generic best-known lower bound  $O(\log q)$  on the clique number that holds for all generalized Paley graphs due to Cohen [4]. In fact, Green [6] showed that the clique number of almost all Cayley graphs

---

*Manuscript received 6th September 2022, revised 8th January 2023, accepted 9th January 2023.*

**KEYWORDS.** Cayley graph, maximal clique, character sum.

**ACKNOWLEDGEMENTS.** The author was supported by a doctoral fellowship from the University of British Columbia.

defined on a cyclic group  $G$  is  $O(\log |G|)$ , as  $|G| \rightarrow \infty$ . While in the case of generalized Paley graphs, the underlying group may not be cyclic, Green's result still suggests that a clique in a Cayley graph with exceptional size (that is, much larger than  $O(\log q)$ ) tends to have special algebraic structures.

Determining the clique number of (generalized) Paley graphs is widely open in general [5]; we refer to [11, Section 1.3] for a survey on recent (minor) improvements on the square root trivial upper bound. Thus, it is interesting if one can show that the above subfield constructions of cliques are not maximal so that the lower bound on the clique number can be further improved. However, the rigid algebraic structure of subfields suggests that it is very unlikely. Indeed, in [12, Conjecture 1.4], Yip conjectured that such constructions give rise to maximal cliques:

**CONJECTURE 1.1** ([12, Conjecture 1.4]). *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  $d \mid \frac{q-1}{p^r-1}$ . Then the subfield  $\mathbb{F}_{p^r}$  forms a maximal clique in  $GP(q, d)$ .*

In other words, the conjecture states that if  $\mathbb{F}_{p^r}$  is the maximum subfield of  $\mathbb{F}_q$  that forms a clique in  $GP(q, d)$ , then in fact it forms a maximal clique. The motivation of Conjecture 1.1 is explained in [12] in greater details; in particular, Yip [12, Section 3] showed that if  $\mathbb{F}_{p^r}$  is not maximal, then there is a clique that is a 2-dimensional space over  $\mathbb{F}_{p^r}$  and consequently the lower bound on the clique number can be improved significantly to  $\omega(GP(q, d)) \geq p^{2r}$ . This observation, together with known upper bounds on the clique number, allows Yip [12, Theorem 1.5 and Theorem 1.6] to confirm Conjecture 1.1 for cubic Paley graphs with cubic order and quadruple Paley graphs with quartic order. However, a similar argument fails to work in general since the best-known upper bound on the clique number is  $O(\sqrt{q})$ .

In this paper, we use different ideas to resolve Conjecture 1.1. For simplicity, we call a clique  $C$  in a Cayley graph  $X = \text{Cay}(\mathbb{F}_q^+, S)$  a *subfield clique* if  $C$  is a subfield of  $\mathbb{F}_q$ , and we say  $C$  is a *maximal subfield clique* if  $C$  is not contained in a strictly larger subfield clique. Our first main result confirms Conjecture 1.1 in a stronger form: a maximal subfield clique in a generalized Paley graph is a maximal clique.

**THEOREM 1.2.** *Let  $d > 1$  be an integer. Let  $q$  be a prime power with  $q^n \equiv 1 \pmod{2d}$  and  $q > (n - 1)^2$ . If  $\mathbb{F}_q$  is a maximal subfield clique in  $GP(q^n, d)$ , then  $\mathbb{F}_q$  is also a maximal clique.*

In [12, Theorem 1.7], Yip described a similar phenomenon in Peisert graphs and conjectured that  $\mathbb{F}_q$  forms a maximal clique in a Peisert graph with order  $q^4$  provided that  $q > 3$ ; this was confirmed by Asgarli and Yip in [1, Theorem 1.5]. Moreover, in [1, Section 5] of the same paper, they observed that a similar result holds for generalized Peisert graphs under extra assumptions.

Our second main result improves and extends the results in [1, Section 5] substantially. Before stating that, we shall recall the definition of generalized Peisert graphs, first introduced by Mullin [9]. This definition is motivated by the similarity between generalized Paley graphs and Peisert graphs (first introduced by Peisert in [10] in order to classify self-complementary symmetric graphs).

**DEFINITION 1.3** ([1, Definition 2.11]). Let  $d$  be a positive even integer, and  $q$  a prime power such that  $q \equiv 1 \pmod{2d}$ . The  $d$ -th power Peisert graph of order  $q$ , denoted  $GP^*(q, d)$ , is the Cayley graph  $\text{Cay}(\mathbb{F}_q^+, M_{q,d})$ , where

$$M_{q,d} = \left\{ g^{dk+j} : 0 \leq j \leq \frac{d}{2} - 1, k \in \mathbb{Z} \right\},$$

and  $g$  is a primitive root of  $\mathbb{F}_q$ .

While the definition of  $GP^*(q, d)$  depends on the choice of the primitive root  $g$ , it is clear that the isomorphism class of  $GP^*(q, d)$  is independent of the choice of  $g$ . We refer to [1, Remark 2.12] for a discussion on the connection between generalized Peisert graphs and generalized Paley graphs. In particular, if  $d$  is even, then  $GP^*(q, d)$  contains  $GP(q, d)$  as a subgraph and thus the structure of maximal cliques in  $GP^*(q, d)$  is potentially richer. However, our second main result shows that a maximal subfield clique in  $GP^*(q, d)$  is still a maximal clique.

**THEOREM 1.4.** *Let  $d \geq 4$  be an even integer. Let  $q$  be a prime power such that  $q^n \equiv 1 \pmod{2d}$  and  $q > (n - 1)^2 d^4 / \pi^2 (d - 1)^2$ . If  $\mathbb{F}_q$  is a maximal subfield clique in  $GP^*(q^n, d)$ , then  $\mathbb{F}_q$  is also a maximal clique.*

Note that Theorem 1.4 refines Theorem 1.2 provided that  $q$  is sufficiently large. In fact, we will prove a more general (yet technical) statement for any Cayley graph containing a generalized Paley graph as a subgraph in Proposition 3.1. Before proving our main results, we shall introduce some preliminary tools in Section 2.

## 2. PRELIMINARIES

A *multiplicative character* of  $\mathbb{F}_q$  is a group homomorphism from  $\mathbb{F}_q^*$  to the multiplicative group of complex numbers with modulus 1. For a multiplicative character  $\chi$ , its order  $d$  is the smallest positive integer such that  $\chi^d = \chi_0$ , where  $\chi_0$  is the trivial multiplicative character of  $\mathbb{F}_q$ . We refer to [8, Chapter 5] for a general discussion on estimates on character sums. The following theorem, due to Katz [7], is crucial in our proofs.

**THEOREM 2.1 (Katz).** *Let  $\theta \in \mathbb{F}_{q^n}$  such that  $\mathbb{F}_q(\theta) = \mathbb{F}_{q^n}$ . Let  $\chi$  be a non-trivial multiplicative character of  $\mathbb{F}_{q^n}$ . Then*

$$\left| \sum_{a \in \mathbb{F}_q} \chi(\theta + a) \right| \leq (n - 1)\sqrt{q}.$$

The following definition is helpful for our discussions.

**DEFINITION 2.2** ([1, Definition 2.16]). Let  $\epsilon > 0$ . A set  $M \subset \mathbb{C}$  is said to be  $\epsilon$ -lower bounded if for every integer  $k \in \mathbb{N}$ , and for every choice of  $x_1, x_2, \dots, x_k \in M$ , we have

$$\left| \sum_{j=1}^k x_j \right| \geq \epsilon k.$$

Using trigonometric manipulations, it is not difficult to show the following lemma.

**LEMMA 2.3** ([1, Lemma 4.5]). *Let  $d \geq 4$  be an even integer, and  $\omega = \exp(2\pi i/d)$ . Then the set  $M = \{\omega^j : 0 \leq j \leq d/2 - 1\}$  is  $(\frac{\pi}{d} - \frac{\pi}{d^2})$ -lower bounded.*

## 3. PROOF OF MAIN RESULTS

We will prove a more general statement in the following proposition, and then deduce Theorem 1.2 and Theorem 1.4 as special cases.

**PROPOSITION 3.1.** *Let  $n \geq 2$  be an integer and  $\epsilon > 0$  a real number. Let  $X = \text{Cay}(\mathbb{F}_{q^n}^+, S)$  be a Cayley graph with  $q > (n - 1)^2 / \epsilon^2$ . Assume that there is an integer  $d > 1$ , such that  $X$  contains  $GP(q^n, d)$  as a subgraph and the set  $M = \{\chi(x) : x \in S\}$  is  $\epsilon$ -lower bounded for some multiplicative character  $\chi$  of  $\mathbb{F}_{q^n}$  with order  $d$ . If  $\mathbb{F}_q$  is a maximal subfield clique in  $X$ , then  $\mathbb{F}_q$  is also a maximal clique in  $X$ .*

*Proof.* Assume that  $\mathbb{F}_q$  is not a maximal clique; then we can find  $\theta \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$  such that  $\mathbb{F}_q \cup \{\theta\}$  forms a clique in  $X$ . Thus, by definition, for any  $a \in \mathbb{F}_q$ , we have  $\theta - a \in S$  and  $\chi(\theta - a) \in M$ .

Let  $\mathbb{F}_{q^m}$  be the smallest extension of  $\mathbb{F}_q$  that contains  $\theta$ ; then  $\mathbb{F}_{q^m}$  is necessarily a subfield of  $\mathbb{F}_{q^n}$  and  $m > 1$ . Let  $\chi'$  be the restriction of  $\chi$  on the subfield  $\mathbb{F}_{q^m}$ ; then  $\chi'$  is a multiplicative character of  $\mathbb{F}_{q^m}$ .

Suppose  $\chi'$  is the trivial multiplicative character of  $\mathbb{F}_{q^m}$ ; then  $\chi(x) = 1$  for each  $x \in \mathbb{F}_{q^m}^*$ . This means that each element in  $\mathbb{F}_{q^m}^*$  is a  $d$ -th power in  $\mathbb{F}_{q^m}^*$  and it follows that  $\mathbb{F}_{q^m}^* \subset S$  since  $X$  contains  $GP(q^n, d)$  as a subgraph. In particular,  $\mathbb{F}_{q^m}$  is a subfield clique in  $X$  that is strictly larger than  $\mathbb{F}_q$ , violating the assumption. Thus,  $\chi'$  is a non-trivial multiplicative character of  $\mathbb{F}_{q^m}$ .

Applying Theorem 2.1 to the character  $\chi'$  on the affine line  $\theta + \mathbb{F}_q$  and using the definition that  $M$  is  $\epsilon$ -lower bounded, we obtain that

$$\epsilon q \leq \left| \sum_{a \in \mathbb{F}_q} \chi(\theta + a) \right| = \left| \sum_{a \in \mathbb{F}_q} \chi'(\theta + a) \right| \leq (m - 1)\sqrt{q} \leq (n - 1)\sqrt{q}.$$

Therefore,  $q \leq (n - 1)^2/\epsilon^2$ , contradicting our assumption. This shows that  $\mathbb{F}_q$  is a maximal clique in  $X$ . □

REMARK 3.2. From the proof, it is easy to see that the condition “ $\{\chi(x) : x \in S\}$  is  $\epsilon$ -lower bounded” in the statement of the above proposition can be weakened to  $|\sum_{x \in A} \chi(x)| \geq \epsilon q$  for any  $A \subset S$  with  $|A| = q$ . In other words, if there is  $S' \subset S$  such that  $|S \setminus S'|$  is small and  $\{\chi(x) : x \in S'\}$  is  $\epsilon$ -lower bounded, then we can still conclude that  $\mathbb{F}_q$  is maximal clique provided that  $q$  is sufficiently large.

REMARK 3.3. A result of a similar flavor has appeared in [1, Theorem 1.3] in terms of maximum cliques in the so-called Peisert-type graphs. It generalizes the celebrated Van Lint–MacWilliams’ conjecture (equivalently, Erdős–Ko–Rado theorem for Paley graphs of square order), first proved by Blokhuis [2]. We refer to [1, Section 2] for a historical discussion.

Finally, we prove Theorem 1.2 and Theorem 1.4, and discuss the sharpness of the assumption that  $q$  is sufficiently large in both theorems.

*Proof of Theorem 1.2.* Note that the connection set  $S$  of  $GP(q^n, d)$  consists of  $d$ -th powers in  $\mathbb{F}_{q^n}^*$ . It follows that  $M = \{\chi(x) : x \in S\} = \{1\}$  is 1-lower bounded for any multiplicative character  $\chi$  of  $\mathbb{F}_{q^n}$  with order  $d$ . Thus, the theorem follows immediately from Proposition 3.1. □

REMARK 3.4. We conjecture that the condition  $q > (n - 1)^2$  in Theorem 1.2 can be dropped. However, we do not know how to remove this condition. When  $n \leq 5$ , we verified that Theorem 1.2 holds for all  $q \leq (n - 1)^2$  by enumerating all possible generalized Paley graphs via SageMath. We also verified that Theorem 1.2 holds for all  $q \leq 17$  when  $n = 6$ .

*Proof of Theorem 1.4.* Let  $g$  be the primitive root of  $\mathbb{F}_{q^n}$  that defines the graph  $GP^*(q^n, d)$ . Let  $\chi$  be a multiplicative character in  $\mathbb{F}_q$  such that  $\chi(g) = \omega$ , where  $\omega = \exp(2\pi i/d)$ ; then  $\chi$  has order  $d$ . As discussed before,  $GP^*(q^n, d)$  contains  $GP(q^n, d)$  as a subgraph. Let  $M = \{\chi(x) : x \in S\}$ , where  $S = \{g^{j+kd} : 0 \leq j \leq d/2 - 1, k \in \mathbb{Z}\}$  is the connection set of  $GP^*(q^n, d)$ . It then follows from Lemma 2.3 that the set

$M = \{\omega^j : 0 \leq j \leq d/2 - 1\}$  is  $(\frac{\pi}{d} - \frac{\pi}{d^2})$ -lower bounded. Therefore, by Proposition 3.1,  $\mathbb{F}_q$  is a maximal clique provided that

$$q > \frac{(n-1)^2}{(\frac{\pi}{d} - \frac{\pi}{d^2})^2} = \frac{(n-1)^2 d^4}{\pi^2 (d-1)^2}.$$

□

REMARK 3.5. We believe that the condition  $q > (n-1)^2 d^4 / \pi^2 (d-1)^2$  in Theorem 1.4 is not optimal. However, we do need to assume  $q$  is sufficiently large for Theorem 1.4 to hold. There are plenty of counterexamples when  $q$  is small compared to  $n$  and  $d$ . For example, when  $q = 3, n = 4$ , and  $d = 4$ , the subfield  $\mathbb{F}_3$  is a maximal subfield clique in  $GP^*(81, 4)$ , and yet there is a maximal clique with size 9 containing  $\mathbb{F}_3$ . Similarly, when  $q = 5, n = 6$ , and  $d = 62$ , the subfield  $\mathbb{F}_5$  is a maximal subfield clique in  $GP^*(15625, 62)$ , and yet there is a maximal clique with size 25 containing  $\mathbb{F}_5$ .

*Acknowledgements.* The author thanks Shamil Asgarli for many helpful discussions.

#### REFERENCES

- [1] Shamil Asgarli and Chi Hoi Yip, *Van Lint–MacWilliams’ conjecture and maximum cliques in Cayley graphs over finite fields*, J. Combin. Theory Ser. A **192** (2022), article no. 105667 (23 pages).
- [2] A. Blokhuis, *On subsets of  $\text{GF}(q^2)$  with square differences*, Nederl. Akad. Wetensch. Indag. Math. **46** (1984), no. 4, 369–372.
- [3] I. Broere, D. Döman, and J. N. Ridley, *The clique numbers and chromatic numbers of certain Paley graphs*, Quaestiones Math. **11** (1988), no. 1, 91–93.
- [4] Stephen D. Cohen, *Clique numbers of Paley graphs*, Quaestiones Math. **11** (1988), no. 2, 225–231.
- [5] Ernest S. Croot, III and Vsevolod F. Lev, *Open problems in additive combinatorics*, in Additive combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 207–233.
- [6] Ben Green, *Counting sets with small sumset, and the clique number of random Cayley graphs*, Combinatorica **25** (2005), no. 3, 307–326.
- [7] Nicholas M. Katz, *An estimate for character sums*, J. Amer. Math. Soc. **2** (1989), no. 2, 197–200.
- [8] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn.
- [9] Natalie Mullin, *Self-complementary arc-transitive graphs and their imposters*, Master’s thesis, University of Waterloo, 2009, <https://uwspace.uwaterloo.ca/handle/10012/4264>.
- [10] Wojciech Peisert, *All self-complementary symmetric graphs*, J. Algebra **240** (2001), no. 1, 209–229.
- [11] Chi Hoi Yip, *Gauss sums and the maximum cliques in generalized Paley graphs of square order*, Funct. Approx. Comment. Math. **66** (2022), no. 1, 119–138.
- [12] ———, *On maximal cliques of Cayley graphs over fields*, J. Algebraic Combin. **56** (2022), no. 2, 323–333.

CHI HOI YIP, Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver V6T 1Z2, Canada  
*E-mail* : kyleyip@math.ubc.ca