Van Lint–MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields

Chi Hoi Yip

University of British Columbia

(Joint work with Shamil Asgarli)

Carleton Combinatorics Meeting 2021
Aug 5, 2021

Direction results revisited

We have seen that Rédei's polynomials and lacunary polynomials are useful tools to study the direction set.

Theorem (Rédei, 1973; Szőnyi,1996)

Let p be a prime, and let $U \subset AG(2, p)$ with $1 < |U| \leq p$. Then either U is contained in a line, or U determines at least $\frac{|U|+3}{2}$ directions.

Observation

A "typical" point set determines many directions. Conversely, a set determining few directions must have some "hidden geometric structure".

Direction results over a general finite field

Question

What about $U \subset AG(2, q)$, where q is an odd prime power?

We expect similar results, but we have to be more careful:

- Subfield obstruction: $U \subset AG(2, q')$, where $\mathbb{F}_{q'}$ is a proper subfield of $\mathbb{F}_q$.
- Subspace obstruction: U has an subspace structure.

Theorem (Ball, 2003)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be any function such that $f(0) = 0$, where q is an odd prime power. Let N be the number of directions determined by the graph of f. If $N < \frac{q+3}{2}$, then there is a subfield K of $\mathbb{F}_q$ such that the graph of f is K-linear.

Van Lint–MacWilliams' Conjecture

Conjecture (van Lint, MacWilliams, 1978)

If A is a subset of $\mathbb{F}_{q^2}$ such that $0, 1 \in A$, $|A| = q$, and $a - b$ is a square for each $a, b \in A$, then A is the subfield $\mathbb{F}_q$.

Definition

Given an abelian group G and a connection set $S \subset G \setminus \{0\}$ with $S = -S$, the Cayley graph $\mathrm{Cay}(G, S)$ is the graph whose vertices are elements of G, such that two vertices g and h are adjacent if and only if $g - h \in S$.

Conjecture (van Lint–MacWilliams' Conjecture reformulated)

In the Paley graph of order q^2, that is $\mathrm{Cay}(\mathbb{F}_{q^2}^+, (\mathbb{F}_{q^2}^*)^2)$, the only maximum clique containing $0, 1$ is the subfield $\mathbb{F}_q$.

Erdős-Ko-Rado property of Paley graphs

Theorem (Blokhuis, 1984; Bruen and Fisher, 1991; Asgarli and Y., 2021)

In the Paley graph of order q^2, the only maximum clique containing $0, 1$ is the subfield $\mathbb{F}_q$.

- This is also known as the Erdős-Ko-Rado property of Paley graphs in the sense that it implies that the only maximum cliques are those canonical cliques: each maximum clique is given by an affine transformation of the subfield $\mathbb{F}_q$.
- Refer to the book *Erdős-Ko-Rado theorems: algebraic approaches* by Godsil and Meagher for a two-step proposal to prove the theorem using the ratio bound. Partial progress in this direction was recently made by Goryainov and Lin.

Van Lint–MacWilliams' conjecture: variants and generalizations

Theorem (Sziklai, 1999)

If q is an odd prime power and d is a divisor of $(q+1)$ such that $d>1$, then in the generalized Paley graph $GP(q^2,d)=\mathrm{Cay}(\mathbb{F}_{q^2}^+,(\mathbb{F}_{q^2}^*)^d)$, the only maximum clique containing $0,1$ is the subfield $\mathbb{F}_q$.

The condition that $d \mid (q+1)$ is necessary: it guarantees that the subfield $\mathbb{F}_q$ forms a clique in $GP(q^2,d)$.

Conjecture (Mullin, 2009)

Let $q \equiv 3 \pmod 4$ be a prime power. Then the only maximum clique containing $0,1$ in the Peisert graph of order q^2 is given by the subfield $\mathbb{F}_q$.

Peisert graphs are similar to Paley graphs in many aspects, but little is known about the structure of their cliques.

Peisert graphs and generalized Peisert graphs

Definition (Peisert, 2001)

The Peisert graph *of order* $q = p^r$*, where* p *is a prime such that* $p \equiv 3 \pmod 4$ *and* r *is even, denoted* P_q^**, is the Cayley graph* $\mathrm{Cay}(\mathbb{F}_q^+, M_q)$ *with* $M_q = \{g^j : j \equiv 0, 1 \pmod 4\}$*, where* g *is a primitive root of the field* $\mathbb{F}_q$*.*

Definition (Mullin, 2009)

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* $\mathrm{Cay}(\mathbb{F}_q^+, M_{q,d})$*, where*

$$M_{q,d} = \left\{ g^j : j \equiv 0, 1, \cdots, \frac{d}{2} - 1 \pmod d \right\},$$

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

Definition (Peisert-type graphs)

Let q be an odd prime power. Let $S \subset \mathbb{F}_{q^2}^*$ be a union of at most $\frac{q+1}{2}$ cosets of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^2}^*$ such that $\mathbb{F}_q^* \subset S$, i.e.,

$$S = c_1\mathbb{F}_q^* \cup c_2\mathbb{F}_q^* \cup \cdots \cup c_m\mathbb{F}_q^*, \tag{1}$$

where $c_1 = 1$ and $m \leq \frac{q+1}{2}$. Then the Cayley graph $X = \mathrm{Cay}(\mathbb{F}_{q^2}^+, S)$ is said to be a Peisert-type graph.

Lemma

The following families of Cayley graphs are Peisert-type graphs:

- *Paley graphs of square order;*
- *Peisert graph with order q^2, where $q \equiv 3 \pmod 4$;*
- *Generalized Paley graphs $GP(q^2, d)$, where $d \mid (q+1)$ and $d > 1$;*
- *Generalized Peisert graphs $GP^*(q^2, d)$, where $d \mid (q+1)$ and d is even.*

Main result

Theorem (Asgarli and Y., 2021)

The Erdős-Ko-Rado property of Paley graphs extends to Peisert-type graphs under some minor assumptions.

In other words, for a Peisert-type graph $X = \mathrm{Cay}(\mathbb{F}_{q^2}^+, S)$, under some assumptions, we can conclude that the only maximum clique containing $0, 1$ is the subfield $\mathbb{F}_q$.

Step 1: show that each maximum clique has subspace structure

Theorem (Asgarli and Y., 2021)

Let X be a Peisert-type graph of order q^2, where q is a power of an odd prime p. Then $\omega(X) = q$, and any maximum clique in X containing 0 is an $\mathbb{F}_p$-subspace of $\mathbb{F}_{q^2}$.

Recall the connection set of X is a union of at most $\frac{q+1}{2}$ cosets of $\mathbb{F}_q^*$. We find a suitable base to embed a maximum clique C to $AG(2,q)$, such that each coset in the connection set contributes to at most one direction.

Theorem (Ball, 2003)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be any function such that $f(0) = 0$, where q is an odd prime power. Let N be the number of directions determined by the graph of f. If $N < \frac{q+3}{2}$, then there is a subfield K of $\mathbb{F}_q$ such that the graph of f is K-linear.

Step 2: show that the subspace must be the subfield

We need to detect whether an $\mathbb{F}_p$-subspace of $\mathbb{F}_{q^2}$ is the subfield $\mathbb{F}_q$. One such tool is character sum estimates. Typically we expect there is a lot of cancellation for a character sum over a subspace, however for a subfield there might be no cancellation at all since the restriction of the character to the subfield might be trivial.

Theorem

Let n be an integer such that $n \geq 2$, and q an odd prime power. Let $\mathcal{V} \subseteq \mathbb{F}_{q^{2n}}$ be an $\mathbb{F}_q$-space of dimension n, with $1 \in \mathcal{V}$, and $\mathcal{V} \neq \mathbb{F}_{q^n}$. Then for any non-trivial multiplicative character χ of $\mathbb{F}_{q^{2n}}$,

$$\left|\sum_{x \in \mathcal{V}} \chi(x)\right| < \frac{2n}{\sqrt{q}} \cdot |\mathcal{V}|. \tag{2}$$

This is a consequence of the character sum estimates by Katz (1989) and Reis (2020).

Formal statement of the main result

Theorem (Asgarli and Y., 2021)

Let $n \geq 2$ be an integer and $\varepsilon > 0$ a real number. Let $X = \mathrm{Cay}(\mathbb{F}_{q^2}^+, S)$ be a Peisert-type graph, where $q = p^n$ and $p > 4.1n^2/\epsilon^2$. Suppose that there is a nontrivial multiplicative character χ of $\mathbb{F}_{q^2}$, such that the set $\{\chi(x) : x \in S\}$ is ε-lower bounded. Then in the Cayley graph X, the only maximum clique containing $0, 1$ is the subfield $\mathbb{F}_q$.

- Roughly speaking, a set A is ε-lower bounded if the sum over any subset of A is not too small.
- The assumption that p is sufficiently large is necessary, we have some counterexamples for generalized Peisert graphs $GP^*(q^2, q+1)$.

Application to Paley graphs and Peisert graphs

- Let χ be the quadratic character, we recover (a slightly weaker version of) van Lint–MacWilliams' conjecture.
- It is worthwhile to remark that all known proofs of the conjecture relied heavily on the fact that the connection set is closed under multiplication.
- Note that for a Peisert graph, the connection set $S = \{g^k : k \equiv 0, 1 \pmod 4\}$ is not closed under multiplication since $g \cdot g = g^2 \notin S$.
- Let χ be a character with order 4, we show (a slightly weaker version of) Mullin's conjecture is true.

Theorem (Asgarli and Y., 2021)

Let $q \equiv 3 \pmod 4$ be a prime power. Let $q = p^n$ for some $n \geq 1$. Assume that $p > 8.2n^2$. Then the only maximum clique containing $0, 1$ in the Peisert graph of order q^2 is given by the subfield $\mathbb{F}_q$.

Thank you for your attention!