Triple intersection numbers for the Paley graphs

Andries E. Brouwer — aeb@cwi.nl
William J. Martin* — martin@wpi.edu

2021-09-05

Abstract

We give a tight bound for the triple intersection numbers of Paley graphs. In particular, we show that any three vertices have a common neighbor in Paley graphs of order larger than 25.

Let $q = 4t + 1$ be a prime power, and let Γ be Paley(q), the Paley graph on q vertices, with as vertex set the finite field $\mathbb{F}_q$ of size q, where two vertices are adjacent when their difference belongs to $\mathbb{F}_q^{*2}$, the set of nonzero squares in $\mathbb{F}_q$. This graph is connected with diameter 2, and self-complementary.

In [5], the authors needed the fact that any function $\psi : \mathbb{F}_q^{*2} \cup \{0\} \to \mathbb{C}^*$ satisfying *(i)* $\psi(0) = 1$ and *(ii)* $\psi(a)\psi(b) = \psi(c)\psi(d)$ whenever $a + b = c + d$ must be the restriction of some additive character of $\mathbb{F}_q$ if $q > 5$. The present note provides a short proof of that fact.

Following the notation of [2] §3, define *generalized intersection numbers* $\left[\begin{smallmatrix} a_1 & a_2 & \cdots & a_\ell \\ i_1 & i_2 & \cdots & i_\ell \end{smallmatrix}\right]$ for $a_1, \ldots, a_\ell \in \mathbb{F}_q$ and $i_1, \ldots, i_\ell \in \{0, 1, 2\}$ by $\left[\begin{smallmatrix} a_1 & a_2 & \cdots & a_\ell \\ i_1 & i_2 & \cdots & i_\ell \end{smallmatrix}\right] := |\Gamma_{i_1}(a_1) \cap \cdots \cap \Gamma_{i_\ell}(a_\ell)|$, where $\Gamma_i(a)$ denotes the set of vertices at distance i from a. Note that $\sum_{i_\ell} \left[\begin{smallmatrix} a_1 & \cdots & a_\ell \\ i_1 & \cdots & i_\ell \end{smallmatrix}\right] = \left[\begin{smallmatrix} a_1 & \cdots & a_{\ell-1} \\ i_1 & \cdots & i_{\ell-1} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} a \\ i \end{smallmatrix}\right] = \frac{q-1}{2}$ and $\left[\begin{smallmatrix} a & b \\ i & j \end{smallmatrix}\right] = \frac{q-1}{4} - \delta_{hi}\delta_{hj}\delta_{ij}$ for distinct a, b and $h, i, j = 1, 2$ where h is the distance from a to b. It follows that all $\left[\begin{smallmatrix} a & b & c \\ h & i & j \end{smallmatrix}\right]$ are known if one knows $\left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right]$.

Proposition 0.1 $\left| \left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right] - \frac{q-9}{8} \right| \le \frac{1}{4}\sqrt{q} + \frac{3}{4}$ *for any three distinct* a, b, c.

Proof. Let χ be the quadratic character. If a, b, c are distinct, then

$$\sum_x (1 + \chi(x-a))(1 + \chi(x-b))(1 + \chi(x-c)) = 8 \left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right] + 4R$$

where $R = \left[\begin{smallmatrix} a & b & c \\ 0 & 1 & 1 \end{smallmatrix}\right] + \left[\begin{smallmatrix} a & b & c \\ 1 & 0 & 1 \end{smallmatrix}\right] + \left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 0 \end{smallmatrix}\right]$, so that $R \in \{0, 1, 3\}$. Let $S = \sum_x \chi((x-a)(x-b)(x-c))$. Since $\sum_x 1 = q$ and $\sum_x \chi(x) = 0$ and $\sum_x \chi(x(x-a)) = -1$ for nonzero a, we see that $q - 3 + S = 8 \left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right] + 4R$.

By Hasse [4], the number of points N on an elliptic curve over $\mathbb{F}_q$ satisfies $|N - (q+1)| \le 2\sqrt{q}$. Consider the curve $y^2 = (x-a)(x-b)(x-c)$. The homogeneous form is $Y^2 Z = (X - aZ)(X - bZ)(X - cZ)$ with a single point $(0, 1, 0)$ at infinity. If $(x-a)(x-b)(x-c)$ is zero for 3 values of x, a nonzero square for m values of x, and a nonsquare for the remaining $q - 3 - m$ values of x, then $N = 1 + 3 + 2m$ and $S = m - (q - 3 - m) = 2m + 3 - q$. Hence $|S| = |N - (q+1)| \le 2\sqrt{q}$. It follows that $\left| \left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right] - \frac{q-9}{8} \right| \le \frac{1}{4}\sqrt{q} + \frac{3}{4}$. □

*Worcester Polytechnic Institute, Dept. of Mathematical Sciences, Worcester, MA USA

Corollary 0.2 *If $q > 25$ then any three distinct vertices in Γ have a common neighbor.* $\square$

The table below gives for small q the values of $[h\,i\,j] := \left[\begin{smallmatrix} a & b & c \\ h & i & j \end{smallmatrix}\right]$ that occur. For each q, the first line is for triangles abc, the second line for paths of length 2. The remaining cases follow by complementation.

q	[1 1 1]	[1 1 2]	[1 2 2]	[2 2 2]
5	-	-	-	-
	0	0	2	0
9	0	0	6	0
	0	3	2	1
13	0	3	6	1
	0–1	3–6	2–5	1–2

q	[1 1 1]	[1 1 2]	[1 2 2]	[2 2 2]
17	0	6	6	2
	1–2	3–6	5–8	1–2
25	0–2	6–12	6–12	2–4
	2–3	6–9	8–11	2–3
29	2	9	12	3
	2–4	6–12	8–14	2–4

Returning to the problem in the second paragraph, if $\psi\colon \mathbb{F}_q^{*2} \cup \{0\} \to \mathbb{C}^*$ satisfies conditions *(i)* and *(ii)*, then $\psi(-a) = \psi(a)^{-1}$ for each a and the extension of ψ to $\hat{\psi}\colon \mathbb{F}_q \to \mathbb{C}^*$ via $\hat{\psi}(a+b) = \psi(a)\psi(b)$ for $a, b \in \mathbb{F}_q^{*2}$, is well-defined. Given $a, b \in \mathbb{F}_q$, we locate c with $c \sim 0, a, -b$ so that $c, a-c, b+c \in \mathbb{F}_q^{*2}$. Now $\hat{\psi}(a+b) = \psi(a-c)\psi(b+c) = \psi(a-c)\psi(c)\psi(-c)\psi(b+c) = \hat{\psi}(a)\hat{\psi}(b)$, showing for $q > 25$ that $\hat{\psi}$ is an additive character. The cases $5 < q \leq 25$ can be done by hand.

In the above, we gave bounds for $\left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right]$, in particular for the number of K_4's on a given triangle abc. In case $q = p$ is prime, a closed formula for the total number of K_4's on a given edge was given by Evans, Pulham & Sheehan [3]. If $p = m^2 + n^2$ where n is odd, this number is $\frac{1}{64}((p-9)^2 - 4m^2)$.

The bounds of Proposition 0.1 are best possible:

Proposition 0.3 *If $q = (4s+1)^2$ for some integer $s \geq 1$, then*
(i) For a suitable triangle abc one has $\left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right] = \frac{q-9}{8} - \frac{1}{4}\sqrt{q} - \frac{3}{4} = 2(s^2-1)$.
(ii) For a suitable cotriangle abc one has $\left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right] = \frac{q-9}{8} + \frac{1}{4}\sqrt{q} + \frac{3}{4} = 2s(s+1)$.

Proof. If abc is a triangle or a cotriangle, then $\left[\begin{smallmatrix} a & b & c \\ 1 & 1 & 1 \end{smallmatrix}\right] + \left[\begin{smallmatrix} a & b & c \\ 2 & 2 & 2 \end{smallmatrix}\right] = \frac{q-9}{4}$. Also, $\left[\begin{smallmatrix} a & b & c \\ 2 & 2 & 2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} ea & eb & ec \\ 1 & 1 & 1 \end{smallmatrix}\right]$ for any nonsquare e. So *(i)* and *(ii)* are equivalent. Let us prove *(i)*, that is, prove that $N = q - 2\sqrt{q} + 1$ occurs for a suitable curve $y^2 = (x-a)(x-b)(x-c)$ where abc is a triangle.

By Waterhouse [6] there are elliptic curves with $N = q \pm 2\sqrt{q} + 1$ points when q is a square. A curve $y^2 = (x-a)(x-b)(x-c)$ has three points of order 2, so 2-torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_2$, so that its number of points is 0 mod 4. Conversely, by Auer & Top [1], given an elliptic curve E with 0 mod 4 points, there is one with the same number of points in Legendre form $y^2 = x(x-1)(x-\lambda)$, except in case $q = r^2$ for a (possibly negative) integer $r \equiv 1 \pmod 4$ when $|E| = (r+1)^2$. Consequently, there is a curve $y^2 = x(x-1)(x-\lambda)$ with $N = (r-1)^2$ points. Then $S = N - (q+1) = -2r$ and $8\left[\begin{smallmatrix} 0 & 1 & \lambda \\ 1 & 1 & 1 \end{smallmatrix}\right] + 4R = N - 4 = (r-1)^2 - 1 = 16s^2 - 4$ and $\left[\begin{smallmatrix} 0 & 1 & \lambda \\ 1 & 1 & 1 \end{smallmatrix}\right] = 2s^2 - \frac{R+1}{2}$. In the extreme cases, E is supersingular (e.g. because $N \equiv 1 \pmod p$) and according to [1] (§3) λ is a square in $\mathbb{F}_{p^2}$, and then also $1 - \lambda$ is a square in $\mathbb{F}_{p^2}$, so that $\{0, 1, \lambda\}$ is a triangle and $R = 3$. $\square$

Acknowledgments

The second author thanks Bill Kantor for helpful remarks. The work of the second author was supported, in part, through a grant from the National Science Foundation (DMS Award #1808376) which is gratefully acknowledged.

References

[1] R. Auer & J. Top, *Legendre curves over finite fields*, J. Number Th. **95** (2002) 303–312.

[2] K. Coolsaet & A. Jurišić, *Using equality in the Krein conditions to prove nonexistence of certain distance-regular graphs*, J. Combin. Th. (A) **115** (2008) 1086–1095.

[3] R. J. Evans, J.R. Pulham & J. Sheehan, *On the number of complete subgraphs contained in certain graphs*, J. Combin. Th. (B) **30** (1981) 364–371.

[4] H. Hasse, *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen*, Nachr. Ges. Wiss. Göttingen, Math.-Phys. K. (1933) 253–262.

[5] W. J. Martin and E. Washock, *On ideals of the eigenpolytopes of Paley graphs and related equiangular lines*, *In preparation*, 2021.

[6] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969) 521–560.