Proof of a Conjecture on Monomial Graphs

Xiang-dong Hou

Department of Mathematics and Statistics
University of South Florida

Joint work with Stephen D. Lappano and Felix Lazebnik

New Directions in Combinatorics

IMS, Singapore, 2016-05-26

outline

- The bipartite graph $G_q(f, g)$ and its background
- The conjecture
- Permutation polynomials
- Previous results
- Outline of a proof of the conjecture
- Open questions

- The bipartite graph $G_q(f, g)$ and its background
- The conjecture
- Permutation polynomials
- Previous results
- Outline of a proof of the conjecture
- Open questions

the bipartite graph $G_q(f,g)$

Let $\mathbb{F}_q$ be the finite field with q elements, q odd. Let $f, g \in \mathbb{F}_q[X, Y]$.

The graph $G = G_q(f,g)$ is an undirected bipartite graph with vertex partitions $P = \mathbb{F}_q^3$ and $L = \mathbb{F}_q^3$, and edges defined as follows: a vertex $(p) = (p_1, p_2, p_3) \in P$ is adjacent to a vertex $[l] = [l_1, l_2, l_3] \in L$ if and only if

$$p_2 + l_2 = f(p_1, l_1) \quad \text{and} \quad p_3 + l_3 = g(p_1, l_1).$$

some graph theory

Let $k \geq 2$, and $g_k(n)$ denote the greatest number of edges in a graph with n vertices and a girth at least $2k+1$. The function $g_k(n)$ has been studied extensively.

Bondy and Simonovits 1974:

$$g_k(n) \leq c_k n^{1+\frac{1}{k}} \quad \text{for } k \geq 2.$$

Lazebnik, Ustimenko and Woldar 1995:

$$g_k(n) \geq \begin{cases} c'_k n^{1+\frac{2}{3k-3+\epsilon}} & \text{if } k \geq 2,\ k \neq 5, \\ c'_5 n^{1+\frac{1}{5}} & \text{if } k = 5, \end{cases}$$

where $\epsilon = 0$ if k is odd, $\epsilon = 1$ if k is even, and c'_k and c_k are positive constants depending on k only.

$$g_k(n) \geq \begin{cases} c'_k n^{1+\frac{2}{3k-3+\epsilon}} & \text{if } k \geq 2,\ k \neq 5, \\ c'_5 n^{1+\frac{1}{5}} & \text{if } k = 5, \end{cases}$$

The only known values of k for which the lower bound for $g_k(n)$ is of magnitude $n^{1+1/k}$, which is the same as the magnitude of the upper bound, are $k = 2, 3$, and 5.

The lower bound for $k = 3$ is given by the graph $G_q(XY, XY^2)$. In fact, $G_q(XY, XY^2)$ has girth 8.

The lower bound for $k = 2, 5$ are given by graphs constructed in a similar manner.

- The bipartite graph $G_q(f, g)$ and its background
- The conjecture
- Permutation polynomials
- Previous results
- Outline of a proof of the conjecture
- Open questions

monomial graphs

When $f, g \in \mathbb{F}_q[X, Y]$ are monomials, the graph $G_q(f, g)$ is called a monomial graph.

We will only consider monomial graphs.

Conjecture 1

Let q be an odd prime power. Then every monomial graph of girth eight is isomorphic to $G_q(XY, XY^2)$.

Theorem

(Dmytrenko, Lazebnik, Williford 2007) Let q be odd. Every monomial graph of girth ≥ 8 is isomorphic to $G_q(XY, X^kY^{2k})$, where $1 \leq k \leq q-1$ is an integer not divisible by p.

The condition that $G_q(XY, X^kY^{2k})$ has girth ≥ 8 implies that certain polynomials are permutations of $\mathbb{F}_q$.

permutation polynomial

A *permutation polynomial* (PP) of $\mathbb{F}_q$ is a polynomial $f \in \mathbb{F}_q[X]$ such that the function defined by $a \mapsto f(a)$ is a bijection on $\mathbb{F}_q$.

A_k and B_k

For an integer $1 \le k \le q-1$, let

$$A_k = X^k\big[(X+1)^k - X^k\big] \in \mathbb{F}_q[X],$$

$$B_k = \big[(X+1)^{2k} - 1\big]X^{q-1-k} - 2X^{q-1} \in \mathbb{F}_q[X].$$

Theorem (DLW 2007)

Let q be odd and $1 \le k \le q-1$ be such that $p \nmid k$. If $G_q(XY, X^kY^{2k})$ has girth ≥ 8, then both A_k and B_k are PPs of $\mathbb{F}_q$.

conjectures on A_k and B_k

Conjecture A (DLW 2007)

Let q be a power of an odd prime p and $1 \le k \le q-1$. Then A_k is a PP of $\mathbb{F}_q$ if and only if k is a power of p.

Conjecture B (DLW 2007)

Let q be a power of an odd prime p and $1 \le k \le q-1$. Then B_k is a PP of $\mathbb{F}_q$ if and only if k is a power of p.

Either of Conjectures A and B implies Conjecture 1.

- The bipartite graph $G_q(f, g)$ and its background
- The conjecture
- Permutation polynomials
- Previous results
- Outline of a proof of the conjecture
- Open questions

prior status of Conjecture 1

For $e > 1$, $\mathrm{gpf}(e)$ = the greatest prime factor of e; $\mathrm{gpf}(1) = 1$.

Theorem (DLW 2007)

Conjecture 1 is true if one of the following occurs.

(i) $q = p^e$, *where* $p \geq 5$ *and* $\mathit{gpf}(e) \leq 3$.

(ii) $3 \leq q \leq 10^{10}$.

Theorem (Kronenthal 2012)

For each prime r *or* $r = 1$, *there is a positive integer* $p_0(r)$ *such that Conjecture 1 is true for* $q = p^e$ *with* $\mathit{gfp}(e) \leq r$ *and* $p \geq p_0(r)$. *In particular, one can choose* $p_0(5) = 7$, $p_0(7) = 11$, $p_0(11) = 13$.

prior status of Conjectures A and B

Theorem (DLW 2007)

Conjecture A is true for $q = p$.

For each odd prime p, let $\alpha(p)$ be the smallest positive even integer a such that

$$\binom{a}{a/2} \equiv (-1)^{a/2} 2^a \pmod{p}.$$

Theorem (Kronenthal 2012)

Let p be an odd prime. If Conjecture B is true for $q = p^e$, then it is also true for $q = p^{em}$ whenever

$$m \le \frac{p-1}{\lfloor (p-1)/\alpha(p) \rfloor}.$$

current status of the conjectures

Lappano, Lazebnik, H 2015

- Conjecture A is true for $q = p^e$, where p is an odd prime and $\text{gpf}(e) \le p - 1$.
- Conjecture B is true for $q = p^e$, where $e > 0$ is arbitrary and p is an odd prime satisfying $\alpha(p) > (p - 1)/2$.
- Conjecture 1 is true.

- The bipartite graph $G_q(f, g)$ and its background
- The conjecture
- Permutation polynomials
- Previous results
- Outline of a proof of the conjecture
- Open questions

strategy

Let q be odd and $1 \le k \le q-1$.

We show that if both A_k and B_k are PPs of $\mathbb{F}_q$, then k is a power of p.

Hermite's criterion

$f \in \mathbb{F}_q[X]$ is a PP of $\mathbb{F}_q$ if and only if

$$\sum_{x\in\mathbb{F}_q} f(x)^s = \begin{cases} 0 & \text{if } 0 \le s \le q-2, \\ -1 & \text{if } s = q-1. \end{cases}$$

power sums of A_k and B_k

For each integer $a > 0$, let $a^* \in \{1, \dots, q-1\}$ be such that $a^* \equiv a \pmod{q-1}$; we also define $0^* = 0$.

For $1 \le s \le q-1$,

$$\sum_{x\in\mathbb{F}_q} A_k(x)^s = (-1)^{s+1}\sum_{i=0}^{s}(-1)^i\binom{s}{i}\binom{(ki)^*}{(2ks)^*},$$

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = -(-2)^s\sum_{i,j}2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)*}{(ki)^*}.$$

criteria for A_k and B_k to be PP

Theorem

(i) *A_k is a PP of $\mathbb{F}_q$ if and only if* $\gcd(k, q-1) = 1$ *and*

$$\sum_i (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*} = 0 \quad \textit{for all } 1 \le s \le q-2.$$

(ii) *B_k is a PP of $\mathbb{F}_q$ if and only if* $\gcd(k, q-1) = 1$ *and*

$$\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{(ks)^*} = (-2)^s \quad \textit{for all } 1 \le s \le q-2.$$

Too much information, too little readily useful. Need to choose suitable s such that useful information can be extracted from the above equations.

notation

Assume that $1 \leq k \leq q-1$ with $\gcd(k, q-1) = 1$.

$$a := \left\lfloor \frac{q-1}{k} \right\rfloor.$$

$k', b \in \{1, \dots, q-1\}$ are such that

$$k'k \equiv 1 \pmod{q-1}, \qquad bk \equiv -1 \pmod{q-1}.$$

$$c := \left\lfloor \frac{q-1}{k'} \right\rfloor.$$

choosing s

Theorem

(i) *A_k is a PP of $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$ and*

$$\sum_i (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*} = 0 \quad \text{for all } 1 \le s \le q-2.$$

(ii) *B_k is a PP of $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$ and*

$$\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{(ks)^*} = (-2)^s \quad \text{for all } 1 \le s \le q-2.$$

choosing s

Theorem

(i) *A_k is a PP of $\mathbb{F}_q$ if and only if gcd$(k, q-1) = 1$ and*

$$\sum_i (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*} = 0 \quad \text{for all } 1 \le s \le q-2.$$

(ii) *B_k is a PP of $\mathbb{F}_q$ if and only if gcd$(k, q-1) = 1$ and*

$$\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{(ks)^*} = (-2)^s \quad \text{for all } 1 \le s \le q-2.$$

- Choose $s = a,\ a-1,\ b,\ q-1-ck',\ q-1-(c-1)k'$, etc.

choosing s

Theorem

(i) *A_k is a PP of $\mathbb{F}_q$ if and only if $gcd(k, q-1) = 1$ and*

$$\sum_i (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*} = 0 \quad \text{for all } 1 \le s \le q-2.$$

(ii) *B_k is a PP of $\mathbb{F}_q$ if and only if $gcd(k, q-1) = 1$ and*

$$\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{(ks)^*} = (-2)^s \quad \text{for all } 1 \le s \le q-2.$$

- Choose $s = a,\ a-1,\ b,\ q-1-ck',\ q-1-(c-1)k'$, etc.
- All but a few terms vanish in the above equations. Useful information is obtained ...

facts about A_k and B_k

Lemma 1

Assume that A_k is a PP of $\mathbb{F}_q$. Then all the base p digits of k' are 0 or 1.

facts about A_k and B_k

Lemma 1

Assume that A_k is a PP of $\mathbb{F}_q$. Then all the base p digits of k' are 0 or 1.

Lemma 2

Assume that all the base p digits of k' are 0 or 1 and k' is not a power of p, then $c \equiv 0 \pmod{p}$.

facts about A_k and B_k

Lemma 1

Assume that A_k is a PP of $\mathbb{F}_q$. Then all the base p digits of k' are 0 or 1.

Lemma 2

Assume that all the base p digits of k' are 0 or 1 and k' is not a power of p, then $c \equiv 0 \pmod{p}$.

Lemma 3

Assume that q is odd, $1 < k \le q-1$, and both A_k and B_k are PPs of $\mathbb{F}_q$. Then c is even and

$$2^{-2ck'} = \binom{2(q-1)-2ck'}{q-1-ck'} + (-1)^{\frac{q-1}{2}+\frac{c}{2}+1}\binom{2(q-1)-2ck'}{\frac{1}{2}(q-1)-(\frac{c}{2}-1)k'}\binom{2c}{c+2}.$$

proof of Conjecture 1

- Assume to the contrary that Conjecture 1 is false. Then there exists $1 \le k \le q-1$, which is not a power of p, such that both A_k and B_k are PPs of $\mathbb{F}_q$.
- Lemma 1 and 2 imply that $c \equiv 0 \pmod{p}$. Then

$$\binom{2c}{c+2} = 0.$$

- Since $q-1-ck' \equiv p-1 \pmod{p}$, the sum $(q-1-ck') + (q-1-ck')$ has a carry in base p at p^0, implying that

$$\binom{2(q-1)-2ck'}{q-1-ck'} = 0.$$

proof of Conjecture 1 — conclusion

Combing

$$2^{-2ck'} =$$
$$\binom{2(q-1)-2ck'}{q-1-ck'} + (-1)^{\frac{q-1}{2}+\frac{c}{2}+1}\binom{2(q-1)-2ck'}{\frac{1}{2}(q-1)-(\frac{c}{2}-1)k'}\binom{2c}{c+2},$$

and
$$\binom{2c}{c+2} = 0 = \binom{2(q-1)-2ck'}{q-1-ck'}$$

gives a contradiction.

- The bipartite graph $G_q(f, g)$ and its background
- The conjecture
- Permutation polynomials
- Previous results
- Outline of a proof of the conjecture
- Open questions

open questions

Conjecture A

Let q be a power of an odd prime p and $1 \le k \le q-1$. Then A_k is a PP of $\mathbb{F}_q$ if and only if k is a power of p.

Conjecture B

Let q be a power of an odd prime p and $1 \le k \le q-1$. Then B_k is a PP of $\mathbb{F}_q$ if and only if k is a power of p.

- Conjecture A is true for $q = p$. Conjecture B has not been established for $q = p$.
- Although Conjectures A and B were originally stated for an odd characteristic, their status also appears to be unsettled for $p = 2$.

Thank You!