On monomial graphs of girth 8.

Vasyl Dmytrenko, Felix Lazebnik, Jason Williford

July 17, 2009

Let $q = p^e$, $f \in \mathbb{F}_q[x]$ is a **permutation** polynomial on $\mathbb{F}_q$ (PP) if

$$c \mapsto f(c)$$

is a bijection of $\mathbb{F}_q$ to $\mathbb{F}_q$.

Examples:

$$ax + b,\ a, b \in \mathbb{F}_q, a \neq 0,$$

$$f = x^p,$$

$$f = x^{p^n}.$$

Conjecture 2:

Let $q = p^e$ be an odd prime power. Then

$$f = (x^2 + x)^k - x^{2k}$$

is a PP on $\mathbb{F}_q$ if and only if $k = p^a$.

Conjecture 2:

Let $q = p^e$ be an odd prime power. Then

$$f = (x^2 + x)^k - x^{2k}$$

is a PP on $\mathbb{F}_q$ if and only if $k = p^a$.

($\Leftarrow$) Obvious.

$$(x^2 + x)^{p^a} - x^{2p^a} = x^{2p^a} + x^{p^a} - x^{2p^a} = x^{p^a},$$

$$c \mapsto c^{p^a} \text{ is a bijection on } \mathbb{F}_q.$$

Conjecture 2:

Let $q = p^e$ be an odd prime power. Then

$$f = (x^2 + x)^k - x^{2k}$$

is a PP on $\mathbb{F}_q$ if and only if $k = p^a$.

($\Leftarrow$) Obvious.

$$(x^2 + x)^{p^a} - x^{2p^a} = x^{2p^a} + x^{p^a} - x^{2p^a} = x^{p^a},$$
$$c \mapsto c^{p^a} \text{ is a bijection on } \mathbb{F}_q.$$

($\Rightarrow$) True for all $q < 10^{10}$.

Let $n \geq 2$, $s \geq 1$.

Generalized n-gon of order r is a bipartite $(r+1)$-regular graph of diameter n and girth $2n$.

Let $n \geq 2$, $s \geq 1$.

Generalized n-gon of order r is a bipartite $(r+1)$-regular graph of diameter n and girth $2n$.

- $r = 1, n \geq 2$: usual C_{2n}.

Let $n \geq 2$, $s \geq 1$.

Generalized n-gon of order r is a bipartite $(r+1)$-regular graph of diameter n and girth $2n$.

- $r = 1, n \geq 2$: usual C_{2n}.
- $r \geq 2, n = 2$: $K_{r+1,r+1}$.

Let $n \geq 2$, $s \geq 1$.

Generalized n-gon of order r is a bipartite $(r+1)$-regular graph of diameter n and girth $2n$.

- $r = 1, n \geq 2$: usual C_{2n}.
- $r \geq 2, n = 2$: $K_{r+1,r+1}$.
- $r \geq 2, n \geq 3$:

Let $n \geq 2$, $s \geq 1$.

Generalized n-gon of order r is a bipartite $(r+1)$-regular graph of diameter n and girth $2n$.

- $r = 1, n \geq 2$: usual C_{2n}.
- $r \geq 2, n = 2$: $K_{r+1,r+1}$.
- $r \geq 2, n \geq 3$:

Tits(59): For $n = 3, 4, 6$, and each prime power r, there exists a generalized n-gon of order r.

Let $n \geq 2$, $s \geq 1$.

Generalized n-gon of order r is a bipartite $(r+1)$-regular graph of diameter n and girth $2n$.

- $r = 1, n \geq 2$: usual C_{2n}.
- $r \geq 2, n = 2$: $K_{r+1,r+1}$.
- $r \geq 2, n \geq 3$:

Tits(59): For $n = 3, 4, 6$, and each prime power r, there exists a generalized n-gon of order r.

Feit-Higman(64): No other values of n are possible.

- A generalized quadrangle of order $r+1$, $GQ(r)$, is a bipartite $(r+1)$-regular graph of diameter 4 and girth 8.

Back

Full Screen

Close

Quit

- A generalized quadrangle of order $r+1$, $GQ(r)$, is a bipartite $(r+1)$-regular graph of diameter 4 and girth 8.
- an $(r+1)$-regular graph of girth 8 with the minimum number of vertices

Back

Full Screen

Close

Quit

- A generalized quadrangle of order $r+1$, $GQ(r)$, is a bipartite $(r+1)$-regular graph of diameter 4 and girth 8.

- an $(r+1)$-regular graph of girth 8 with the minimum number of vertices

  It is easy to show that each partition of $GQ(r)$ contains r^3+r^2+r+1 vertices.

- a bipartite graph of girth 8 with each partition having r^3+r^2+r+1 vertices and with maximum number of edges. Neuwirth(01), Hoory (02)

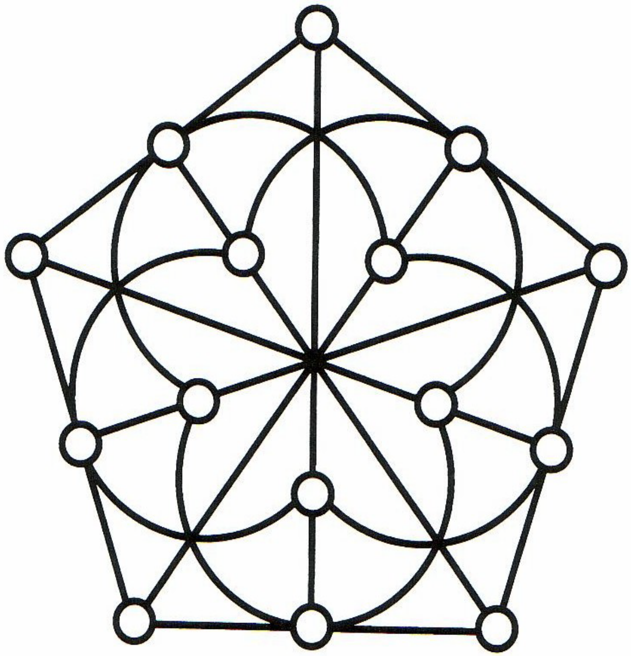
- A generalized quadrangle of order $r+1$, $GQ(r)$, is a bipartite $(r+1)$-regular graph of diameter 4 and girth 8.

- an $(r+1)$-regular graph of girth 8 with the minimum number of vertices

  It is easy to show that each partition of $GQ(r)$ contains r^3+r^2+r+1 vertices.

- a bipartite graph of girth 8 with each partition having r^3+r^2+r+1 vertices and with maximum number of edges. Neuwirth(01), Hoory (02)

- a finite geometry (points and lines) with $r+1$ points on every line, $r+1$ lines passing through every point, and such that for every point x not on a line L there exists a unique line M through x which intersects L.



GQ(2): "Doily"

NO $GQ(r)$ is known if r is not a prime power.

- $GQ(q)$ exists for every prime power q .
- For all but few small even prime powers q, there exist non-isomorphic $GQ(q)$.

NO $GQ(r)$ is known if r is not a prime power.

- $GQ(q)$ exists for every prime power q .
- For all but few small even prime powers q, there exist non-isomorphic $GQ(q)$.
- For odd prime power q, there exist only one generalized 4-gon.

Example of $GQ(q)$

Here are two description of the $GQ(q)$, q odd, by Benson(66).

The first model.

$$\mathbf{Q_4} = \{(x_0, \ldots, x_4) \in \mathbb{F}_q^5 : x_0^2 + x_1 x_2 + x_3 x_4 = 0\}$$

Points and Lines: these are 1- and 2-dimensional totally isotropic subspaces of $\mathbf{Q_4}$, respectively. The adjacency (incidence) is defined by containment. The obtained GQ is denoted by $\mathbf{Q}(4, q)$.

It is known that all nonsingular quadrics in $PG(4, q)$ are projectively equivalent.

The second model. Consider the following bilinear form on $\mathbb{F}_q^4$:

$$\mathbf{x} \cdot \mathbf{y} = y_1 x_0 - y_0 x_1 + y_3 x_2 - y_2 x_3 = 0.$$

Then $x \cdot y = -y \cdot x$, and so $x \cdot x = 0$.

Points and Lines: these are 1- and 2-dimensional totally isotropic subspaces in the symplectic geometry on $\mathbb{F}_q^4$. The adjacency (incidence) is defined by containment. The obtained GQ is denoted by $\mathbf{W}(q)$.

Again, all non-degenerate anti-symmetric bilinear forms on $PG(3, q)$ are projectively equivalent.

The second model. Consider the following bilinear form on $\mathbb{F}_q^4$:

$$\mathbf{x} \cdot \mathbf{y} = y_1 x_0 - y_0 x_1 + y_3 x_2 - y_2 x_3 = 0.$$

Then $x \cdot y = -y \cdot x$, and so $x \cdot x = 0$.

Points and Lines: these are 1- and 2-dimensional totally isotropic subspaces in the symplectic geometry on $\mathbb{F}_q^4$. The adjacency (incidence) is defined by containment. The obtained GQ is denoted by $\mathbf{W}(q)$.

Again, all non-degenerate anti-symmetric bilinear forms on $PG(3, q)$ are projectively equivalent.

****

As incidence geometries, $\mathbf{Q}(4, q)$ and $\mathbf{W}(q)$ are dual of each other. (Benson (70)).
Their point-line incidence bipartite graphs are isomorphic.

None of them is self-dual (Thas(73)).

QUESTION:

Given and ODD prime power q, is there a $GQ(q)$ such that

$$GQ(q) \not\cong \mathbf{Q}(4,q), \quad (\text{or } \mathbf{W}(q)) \,?$$

A Turán-type problem.

What is the greatest number of edges a graph with v vertices can have if its girth at least 8?

$$\Theta(v^{1+1/3}), \quad \text{when} \quad v \longrightarrow \infty.$$

What is the greatest number of edges a graph with v vertices can have if it contains no 6-cycle?

$$\Theta(v^{1+1/3}), \quad \text{when} \quad v \longrightarrow \infty.$$

The asymptotic lower bounds are provided by generalized 4-gons (or their subgraphs).

$GQ(q)$ contains

$$1 + q + q^2 + q^3$$

vertices in each partition.

Let xy be an edge of $GQ(q)$. Remove it and all vertices that are at distance at most 3 from both x and y.

Let $AGQ(q)$ denote the remaining graph, called an an affine part of $GQ(q)$.

Then

1. $AGQ(q)$ is a bipartite q-regular graph of girth 8. Each partition contains q^3 vertices.
2. Diameter of $AGQ(q)$ is 6.

Why is it worth to look at the affine parts?

- $AGQ(q)$ is “CLOSE” to $GQ(q)$: it differs from $GQ(q)$ by “just” a tree with all internal vertices of degree $(q+1)$ and is q-regular graph of the same girth 8. And graph $AGQ(q)$ is simpler.

- $$e \sim 2^{-\frac{4}{3}} v^{1+1/3},\ v \to \infty,$$

  for both $AGQ(q)$ and $GQ(q)$. Hence for the Turán type extremal problems the graphs are equally good.

- For $AGQ(q)$ of the classical $GQ(q)$, there exist relatively simple descriptions.

The only known $GQ(q)$ for odd q has its affine part described as follows. Its partitions are $P = L = \mathbb{F}_q^3$ and for $p \in P$ and $l \in L$,

$$p = (p_1, p_2, p_3) \sim l = [l_1, l_2, l_3] \quad \Leftrightarrow$$

$$\begin{aligned} p_2 + l_2 &= p_1 l_1 \\ p_3 + l_3 &= p_1 l_1^2 \end{aligned}$$

The only known $GQ(q)$ for odd q has its affine part described as follows. Its partitions are $P = L = \mathbb{F}_q^3$ and for $p \in P$ and $l \in L$,

$$p = (p_1, p_2, p_3) \sim l = [l_1, l_2, l_3] \quad \Leftrightarrow$$

$$\begin{aligned} p_2 + l_2 &= p_1 l_1 \\ p_3 + l_3 &= p_1 l_1^2 \end{aligned}$$

We denote this graph by $G(q; xy, xy^2)$.

The only known $GQ(q)$ for odd q has its affine part described as follows. Its partitions are $P = L = \mathbb{F}_q^3$ and for $p \in P$ and $l \in L$,

$$p = (p_1, p_2, p_3) \sim l = [l_1, l_2, l_3] \quad \Leftrightarrow$$

$$p_2 + l_2 = p_1 l_1$$
$$p_3 + l_3 = p_1 l_1^2$$

We denote this graph by $G(q; xy, xy^2)$.
It is easy to check that $G(q; xy, xy^2)$ is a q-regular graph of girth 8.

Problem: Are there two functions $f, g \in \mathbb{F}_q[x, y]$ such that the graph $G(q; f, g)$:

$$p_2 + l_2 = f(p_1, l_1)$$
$$p_3 + l_3 = g(p_1, l_1)$$

has girth 8 and not isomorphic to $G(q; xy, xy^2)$?

Problem: Are there two functions $f, g \in \mathbb{F}_q[x, y]$ such that the graph $G(q; f, g)$:

$$p_2 + l_2 = f(p_1, l_1)$$
$$p_3 + l_3 = g(p_1, l_1)$$

has girth 8 and not isomorphic to $G(q; xy, xy^2)$?

If such a graph exists, it is a candidate for a new $GQ(q)$ which we may try to build from it by "attaching" a tree on $2(1 + q + q^2)$ vertices.

Problem: Are there two functions $f, g \in \mathbb{F}_q[x, y]$ such that the graph $G(q; f, g)$:

$$p_2 + l_2 = f(p_1, l_1)$$
$$p_3 + l_3 = g(p_1, l_1)$$

has girth 8 and not isomorphic to $G(q; xy, xy^2)$?

If such a graph exists, it is a candidate for a new $GQ(q)$ which we may try to build from it by "attaching" a tree on $2(1 + q + q^2)$ vertices.

What conditions should f and g satisfy that the graph $G(q; f, g)$:

$$p_2 + l_2 = f(p_1, l_1)$$
$$p_3 + l_3 = g(p_1, l_1)$$

has girth 8?

Let $\Delta_2(h) : \mathbb{F}_q[x, y] \longrightarrow \mathbb{F}_q[x_1, x_2, y_1, y_2]$ such that

$$h(x, y) \mapsto h(x_1, y_1) - h(x_2, y_1) + h(x_2, y_2) - h(x_1, y_2),$$

and

$\Delta_3(h) : \mathbb{F}_q[x, y] \longrightarrow \mathbb{F}_q[x_1, x_2, x_3, y_1, y_2, y_3]$ such that

$$h(x, y) \mapsto$$

$$h(x_1, y_1) - h(x_2, y_1) + h(x_2, y_2) - h(x_3, y_2) + h(x_3, y_3) - h(x_1, y_3)$$

Theorem. Graph $G(q; f, g)$ contains NO

- 4-cycle if and only if for every solution of the system

$$\begin{aligned} \Delta_2(f) &= 0 \\ \Delta_2(g) &= 0, \end{aligned}$$

$x_1 = x_2$ or $y_1 = y_2$.

- 6-cycle if and only if for every solution of the system

$$\begin{aligned} \Delta_3(f) &= 0 \\ \Delta_3(g) &= 0, \end{aligned}$$

$x_i = x_j$ or $y_i = y_j$ for some distinct $i, j \in \{1, 2, 3\}$.

Monomial graphs

What if we try both f and g to be MONOMIALS in x, y?

Let $G = G(q; x^m y^n, x^u y^v)$, i.e.

$$p_2 + l_2 = p_1^m l_1^n$$
$$p_3 + l_3 = p_1^u l_1^v$$

Why monomials?

For even q, they produce numerous example of non-isomorphic GQ.

For several classes of polynomials, we could show that the girth of G is less than 8. E.g., the girth of

$$G(q; x^m y^n, x^{u_1} y^{v_1} + \lambda x^{u_2} y^{v_2})$$

is 6 for q sufficiently large Dmytrenko-L (05).

Back

Full Screen

Close

Quit

Theorem. Dmytrenko-L.-Williford (FFA, 2007)

Let $q = p^e$ be an odd prime power, and let girth of $G = G(q; x^m y^n, x^u y^v)$ be at least 8. Then

- If $q \geq 5$ and $e = 2^a 3^b$, then $G \cong G(q; xy, xy^2) = AGQ(q)$.

Theorem. Dmytrenko-L.-Williford (FFA, 2007)

Let $q = p^e$ be an odd prime power, and let girth of $G = G(q; x^m y^n, x^u y^v)$ be at least 8. Then

- If $q \geq 5$ and $e = 2^a 3^b$, then $G \cong G(q; xy, xy^2) = AGQ(q)$.
- If $p \geq 5$ and $e \neq 2^a 3^b$, then $G \cong G(q; xy, x^k y^{2k})$, where k satisfies the conditions:

Theorem. Dmytrenko-L.-Williford (FFA, 2007)

Let $q = p^e$ be an odd prime power, and let girth of $G = G(q; x^m y^n, x^u y^v)$ be at least 8. Then

- If $q \geq 5$ and $e = 2^a 3^b$, then $G \cong G(q; xy, xy^2) = AGQ(q)$.
- If $p \geq 5$ and $e \neq 2^a 3^b$, then $G \cong G(q; xy, x^k y^{2k})$, where k satisfies the conditions:

$$1 \leq k < (q-1)/2, \quad \gcd(k, q-1) = 1,$$

$$(2k-1) \not| \, (q-1), \quad k \equiv 1 \pmod{(p-1)},$$

$$\binom{2k}{k} \equiv 2 \pmod{p}, \; \binom{4k}{2k} \equiv 6 \pmod{p},$$

$$f(x) = (x^2 + x)^k - x^{2k} \text{ is a PP on } \mathbb{F}_q$$

etc...

Theorem. Dmytrenko-L.-Williford (FFA, 2007)

Let $q = p^e$ be an odd prime power, and let girth of $G = G(q; x^m y^n, x^u y^v)$ be at least 8. Then

- If $q \geq 5$ and $e = 2^a 3^b$, then $G \cong G(q; xy, xy^2) = AGQ(q)$.
- If $p \geq 5$ and $e \neq 2^a 3^b$, then $G \cong G(q; xy, x^k y^{2k})$, where k satisfies the conditions:

  $$1 \leq k < (q-1)/2, \quad \gcd(k, q-1) = 1,$$

  $$(2k-1) \not| (q-1), \quad k \equiv 1 \pmod{(p-1)},$$

  $$\binom{2k}{k} \equiv 2 \pmod{p}, \ \binom{4k}{2k} \equiv 6 \pmod{p},$$

  $$f(x) = (x^2+x)^k - x^{2k} \text{ is a PP on } \mathbb{F}_q$$

  etc...
- For $3 \leq q \leq 10^{10}$, $G \cong G(q; xy, xy^2) = AGQ(q)$.

Conjecture 1.

Let q be an odd prime power. Then every monomial graph of girth 8 is isomorphic to $G(q; xy, xy^2)$.

Conjecture 2.

Let $q = p^e$ be an odd prime power. Then

$$f(x) = (x^2 + x)^k - x^{2k}$$

is a PP on $\mathbb{F}_q$ if and only if $k = p^a$.

Conjecture 2 $\Rightarrow$ Conjecture 1

Some ideas of the proof.

- Use of automorphisms of monomial graphs $G(q; x^m y^n, x^u y^v)$ to reduce the question to graphs $G(q; xy, x^k y^{2k})$. One element of the reduction was the following result of Matthews (94):

$$1 + x + x^2 + \ldots x^k$$

  is PP if and only if $k \equiv 1 \pmod{p(q-1)}$.

- We observed that graphs $G(q; xy, x^k y^{2k})$ always contain 6-cycles of a special form, and tried to prove it. This is how the question whether the polynomial $(x^2 + x)^k - x^{2k}$ is PP was born.

- For the analysis of $(x^2 + x)^k - x^{2k}$ we used Hermite-Dickson criterium, and some *ad hoc* approaches.

Back
Full Screen
Close
Quit

Problem: Are there three functions $f, g, h \in \mathbb{F}_q[x, y]$ such that the following graph $G(q; f, g, h)$ has no 8-cycle?

For $G(q; f, g, h)$: $p \in \mathbb{F}_q^4$ and $l \in \mathbb{F}_q^4$,

$$p = (p_1, p_2, p_3, p_4) \sim l = [l_1, l_2, l_3, l_4] \quad \Leftrightarrow$$

$$\begin{aligned} p_2 + l_2 &= f(p_1, l_1) \\ p_3 + l_3 &= g(p_1, l_1) \\ p_4 + l_4 &= h(p_1, l_1) \end{aligned}$$

An equivalent form of this problem is:

Are there three functions $f, g, h \in \mathbb{F}_q[x, y]$ such that the system

$$\Delta_4(f) = \Delta_4(g) = \Delta_4(h) = 0$$

has a solution $(x_1, \ldots, x_4, y_1, \ldots, y_4)$ such that $x_i \neq x_{i+1}$, and $y_i \neq y_{i+1}$ for $i = 1, 2, 3, 4$?

Positive answer to this question will solve a 60 year old question on the magnitude of the maximum number of edges in a graph on v vertices and without C_8.

If the answer to the previous question seems to be definite "NO", one should compare it with the following result of Wenger(91), and L.-Ustimenko (93):

Graph $G(q; xy, xy^2, xy^3, xy^4)$

$$p_2 + l_2 = p_1 l_1$$
$$p_3 + l_3 = p_1 l_1^2$$
$$p_4 + l_4 = p_1 l_1^3$$
$$p_5 + l_5 = p_1 l_1^4$$

has no 10-cycles.

This means that every solution $(x_1, \ldots, x_5, y_1, \ldots, y_5)$ of this system

$$\Delta_5(xy) = \Delta_5(xy^2) = \Delta_5(xy^3) = \Delta_5(xy^4) = 0$$

has $x_i = x_{i+1}$ or $y_i \neq y_{i+1}$ for some $i = 1, \ldots, 5$.

Back

Full Screen

Close

Quit