Algebraically defined graphs and generalized quadrangles

Brian Kronenthal

Department of Mathematics
Kutztown University of Pennsylvania

Combinatorics and Computer Algebra 2015
July 22, 2015

Cages and the Moore bound

For given positive integers k and g, find the minimum number of vertices that can be used to construct a k-regular graph of girth g.

Cages and the Moore bound

For given positive integers k and g, find the minimum number of vertices that can be used to construct a k-regular graph of girth g.

A graph with this minimal number of vertices is called a (k, g)-*cage*.

Cages and the Moore bound

For given positive integers k and g, find the minimum number of vertices that can be used to construct a k-regular graph of girth g.

A graph with this minimal number of vertices is called a (k, g)-*cage*.

It is impossible to construct a (k, g)-cage using fewer than

$$\begin{cases} 1 + k\displaystyle\sum_{i=0}^{\frac{g-3}{2}}(k-1)^i = \dfrac{k(k-1)^r - 2}{k-2} & \text{if } g = 2r+1 \\ 2\displaystyle\sum_{i=0}^{\frac{g-2}{2}}(k-1)^i = \dfrac{2(k-1)^r - 2}{k-2} & \text{if } g = 2r \end{cases}$$

vertices.

Cages and the Moore bound

For given positive integers k and g, find the minimum number of vertices that can be used to construct a k-regular graph of girth g.

A graph with this minimal number of vertices is called a (k, g)-*cage*.

It is impossible to construct a (k, g)-cage using fewer than

$$\begin{cases} 1 + k\displaystyle\sum_{i=0}^{\frac{g-3}{2}}(k-1)^i = \dfrac{k(k-1)^r - 2}{k-2} & \text{if } g = 2r+1 \\ 2\displaystyle\sum_{i=0}^{\frac{g-2}{2}}(k-1)^i = \dfrac{2(k-1)^r - 2}{k-2} & \text{if } g = 2r \end{cases}$$

vertices.

This lower bound on the number of vertices is called the **Moore bound**.

Cages and the Moore bound

For given positive integers k and g, find the minimum number of vertices that can be used to construct a k-regular graph of girth g.

A graph with this minimal number of vertices is called a (k, g)-*cage*.

It is impossible to construct a (k, g)-cage using fewer than

$$\begin{cases} 1 + k\displaystyle\sum_{i=0}^{\frac{g-3}{2}}(k-1)^i = \dfrac{k(k-1)^r - 2}{k-2} & \text{if } g = 2r+1 \\ 2\displaystyle\sum_{i=0}^{\frac{g-2}{2}}(k-1)^i = \dfrac{2(k-1)^r - 2}{k-2} & \text{if } g = 2r \end{cases}$$

vertices.

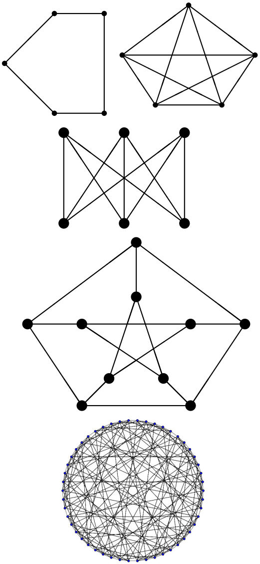
This lower bound on the number of vertices is called the **Moore bound**.

Key idea: It is not always possible to construct a graph that meets the Moore bound.

When can the Moore Bound (potentially) be achieved?

The ONLY possible parameters and examples:

k	g	Unique (k,g)-cage meeting the lower bound
2	g	C_g
k	3	K_{k+1}
k	4	$K_{k,k}$
3	5	Petersen graph
7	5	Hoffman-Singleton graph
57	5	?????
k	6	Incidence graphs of generalized 3-gons of prime power order $k-1$
k	8	Incidence graphs of generalized 4-gons of prime power order $k-1$
k	12	Incidence graphs of generalized 6-gons of prime power order $k-1$



Wikipedia(Uzyel)

Brief intermission: What about a $(57, 5)$-cage?

- A $(57, 5)$-cage would have 3250 vertices and diameter 2.
- The eigenvalues of such a graph's adjacency matrix 57, 7, and -8 (with multiplicities 1, 1729, and 1520, respectively).
- Properties of the automorphism group of a $(57, 5)$-cage have been studied.

What is a Generalized Quadrangle?

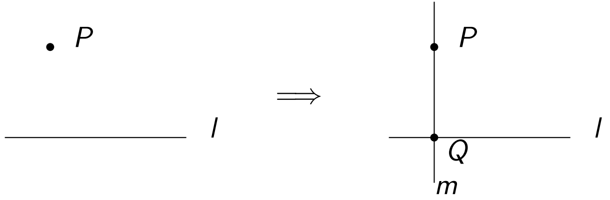
k	g	Unique (k, g)-cage meeting the lower bound
2	g	C_g
k	3	K_{k+1}
k	4	$K_{k,k}$
3	5	Petersen graph
7	5	Hoffman-Singleton graph
57	5	?????
k	6	Incidence graphs of generalized 3-gons of prime power order $k-1$
k	8	**Incidence graphs of generalized 4-gons of prime power order $k-1$**
k	12	Incidence graphs of generalized 6-gons of prime power order $k-1$

What is a Generalized Quadrangle?

Definition

A **generalized quadrangle of order** q is an incidence structure of $q^3 + q^2 + q + 1$ points and $q^3 + q^2 + q + 1$ lines such that...

1. Every point lies on $q + 1$ lines; two distinct points determine at most one line.
2. Every line contains $q + 1$ points; two distinct lines have at most one point in common.
3. If P is a point and L is a line such that P is not on L, then there exists a unique line that contains P and intersects L.

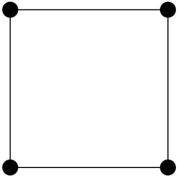


An example: $GQ(1)$

1. Every point lies on two lines; two distinct points determine at most one line.
2. Every line contains two points; two distinct lines have at most one point in common.
3. If P is a point and L is a line such that P is not on L, then there exists a unique line that contains P and intersects L.

An example: $GQ(1)$

1. Every point lies on two lines; two distinct points determine at most one line.
2. Every line contains two points; two distinct lines have at most one point in common.
3. If P is a point and L is a line such that P is not on L, then there exists a unique line that contains P and intersects L.



$GQ(q)$: An alternate characterization

Definition

A **generalized quadrangle of order** q is an incidence structure whose connected (bipartite) point-line incidence graph:

1. is $(q+1)$-regular (every vertex is connected to $q+1$ others)
2. has girth eight (there are no cycles of length less than eight)
3. has diameter four (the distance between any two vertices is at most four)

Example: An alternate characterization of $GQ(1)$

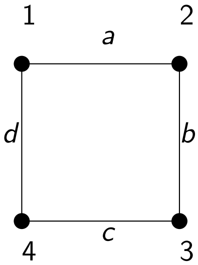
The point-line incidence graph of $GQ(1)$...

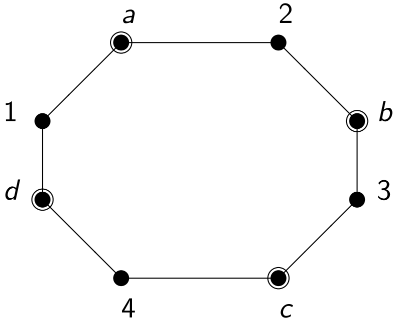
1. is two-regular
2. has girth eight
3. has diameter four

Example: An alternate characterization of $GQ(1)$

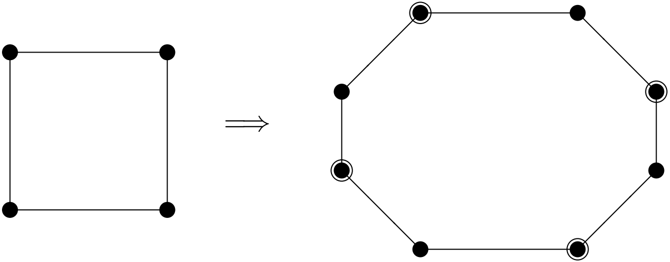
The point-line incidence graph of $GQ(1)$...

1. is two-regular
2. has girth eight
3. has diameter four

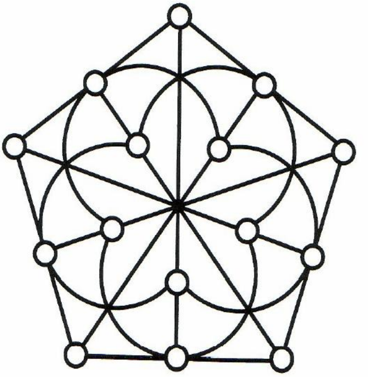




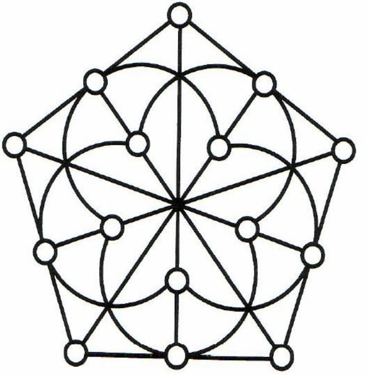
Example: $GQ(1)$



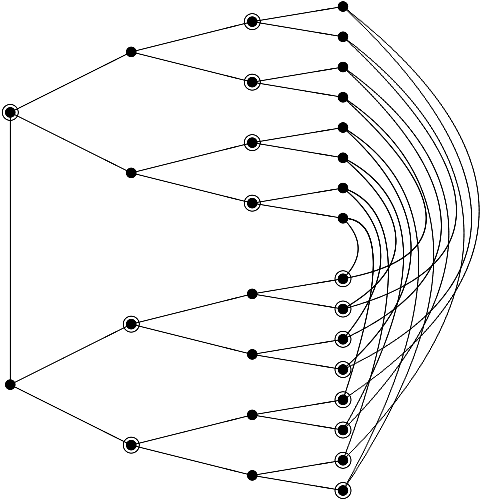
Example: $GQ(2)$



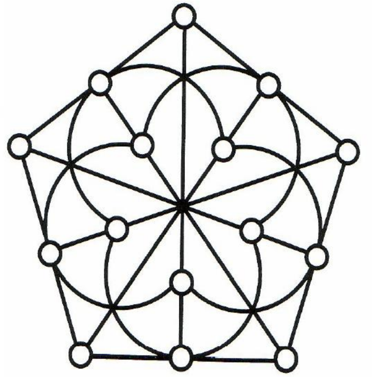
Example: $GQ(2)$



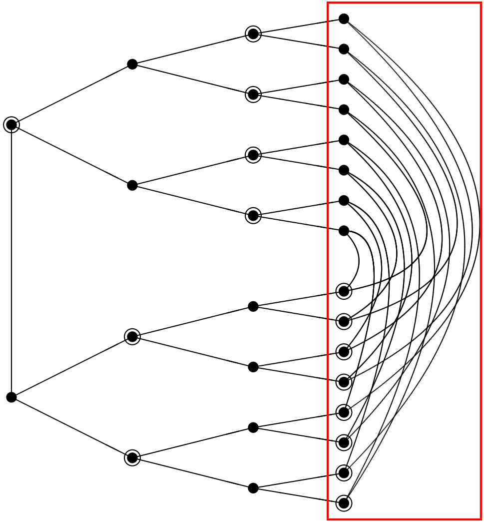
$\Longrightarrow$



Example: $GQ(2)$



$\Longrightarrow$

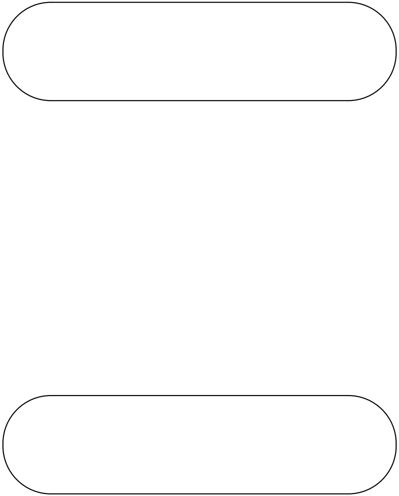


How can we represent this boxed subgraph?

We will construct a family of bipartite graphs as follows.

Let $\mathbb{F}$ be a field.

Let $f(x, y)$ and $g(x, y)$ be bivariate polynomials with coefficients in $\mathbb{F}$.

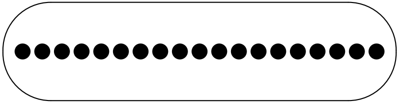


Connection to Algebraically Defined Graphs

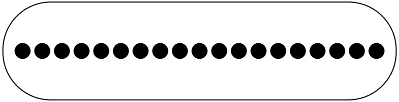
We will construct a family of bipartite graphs as follows.

Let $\mathbb{F}$ be a field.

Let $f(x, y)$ and $g(x, y)$ be bivariate polynomials with coefficients in $\mathbb{F}$.



$P = \mathbb{F}^3 = \{(x_1, x_2, x_3) | x_i \in \mathbb{F}\}$



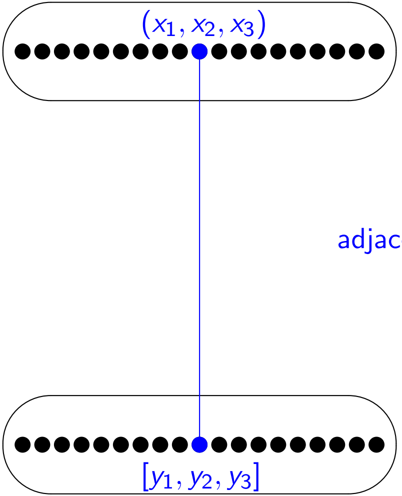
$L = \mathbb{F}^3 = \{[y_1, y_2, y_3] | y_i \in \mathbb{F}\}$

Connection to Algebraically Defined Graphs

We will construct a family of bipartite graphs as follows.

Let $\mathbb{F}$ be a field.

Let $f(x,y)$ and $g(x,y)$ be bivariate polynomials with coefficients in $\mathbb{F}$.



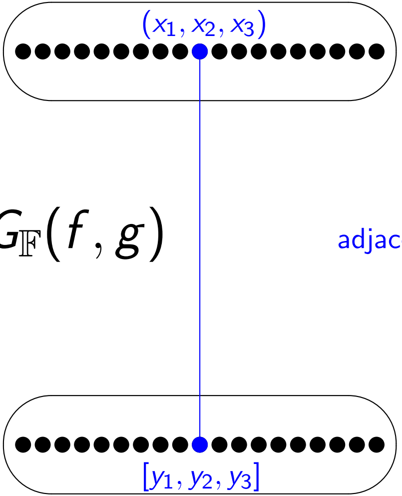
$$P = \mathbb{F}^3 = \{(x_1, x_2, x_3) | x_i \in \mathbb{F}\}$$

$$\text{adjacency iff } \begin{cases} x_2 + y_2 = f(x_1, y_1) \\ x_3 + y_3 = g(x_1, y_1) \end{cases}$$

$$L = \mathbb{F}^3 = \{[y_1, y_2, y_3] | y_i \in \mathbb{F}\}$$

Connection to Algebraically Defined Graphs

We will construct a family of bipartite graphs as follows.
Let $\mathbb{F}$ be a field.
Let $f(x,y)$ and $g(x,y)$ be bivariate polynomials with coefficients in $\mathbb{F}$.



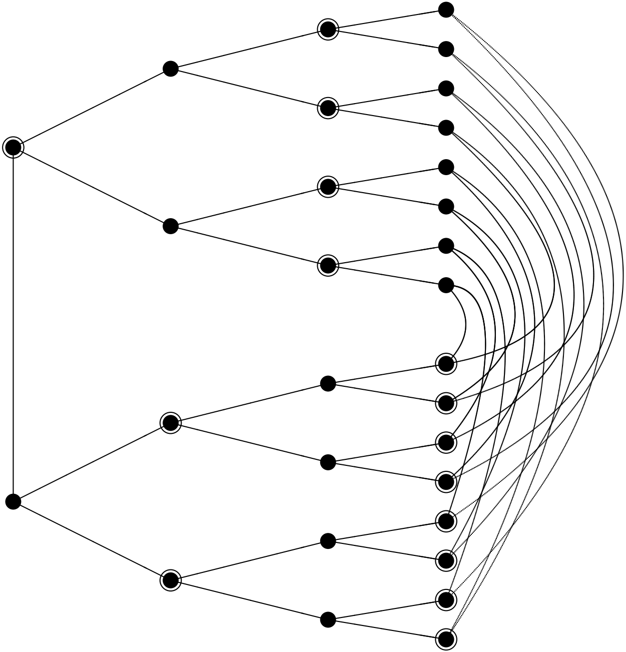
$P = \mathbb{F}^3 = \{(x_1, x_2, x_3) | x_i \in \mathbb{F}\}$

$G_{\mathbb{F}}(f, g)$

adjacency iff $\begin{cases} x_2 + y_2 = f(x_1, y_1) \\ x_3 + y_3 = g(x_1, y_1) \end{cases}$

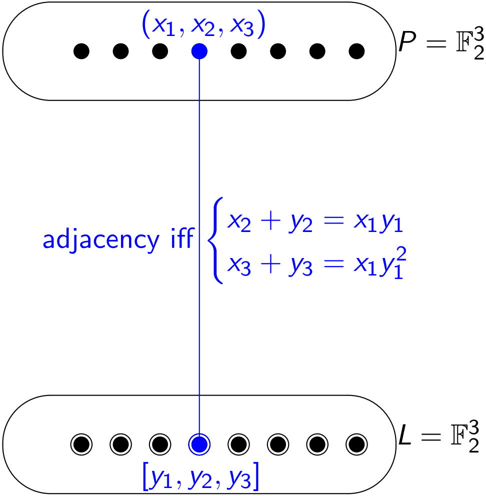
$L = \mathbb{F}^3 = \{[y_1, y_2, y_3] | y_i \in \mathbb{F}\}$

$GQ(2)$

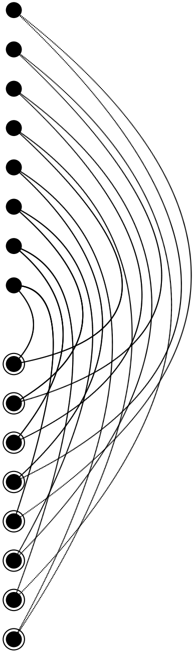


$q = 2$

$G_{\mathbb{F}_2}(xy, xy^2)$

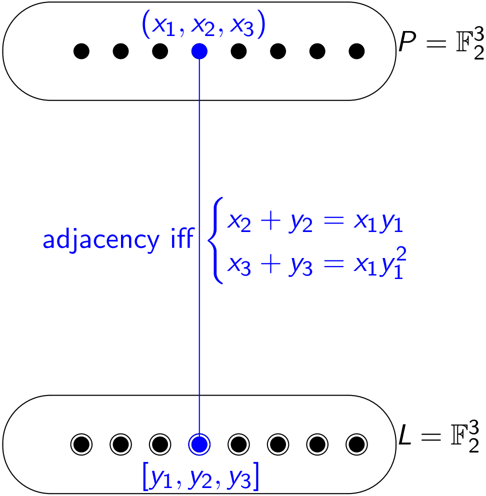


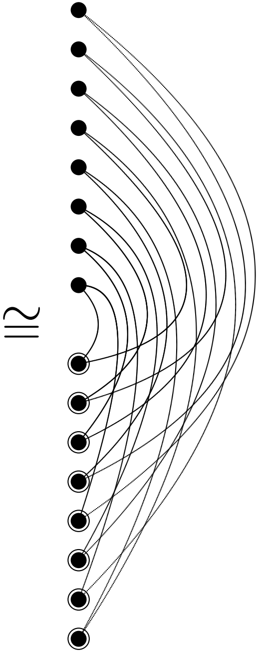
$\cong$



$q = 2$

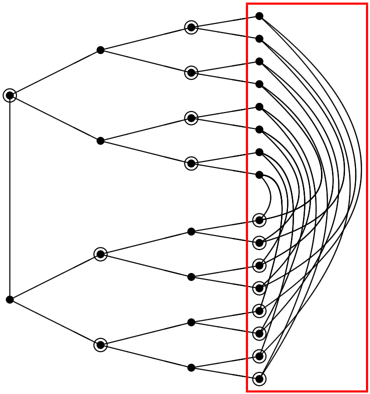
$G_{\mathbb{F}_2}(xy, xy^2)$





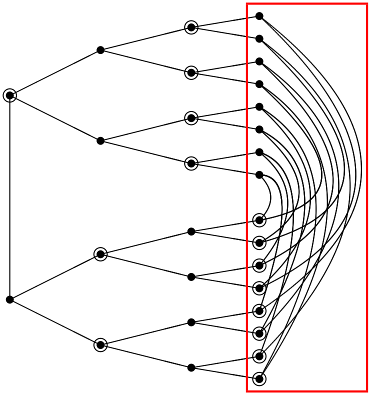
Generalizes to any $\mathbb{F}_q$

Question: Is $G_{\mathbb{F}}(xy, xy^2)$ the unique girth eight algebraically defined graph (up to isomorphism)?



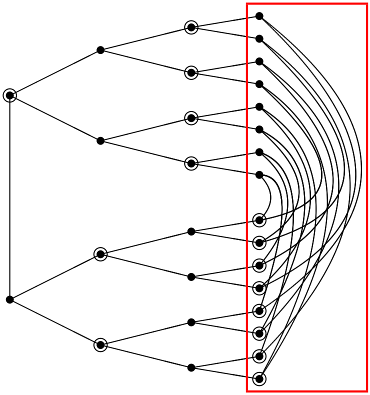
Question: Is $G_{\mathbb{F}}(xy, xy^2)$ the unique girth eight algebraically defined graph (up to isomorphism)?

- If so, we have an interesting characterization.



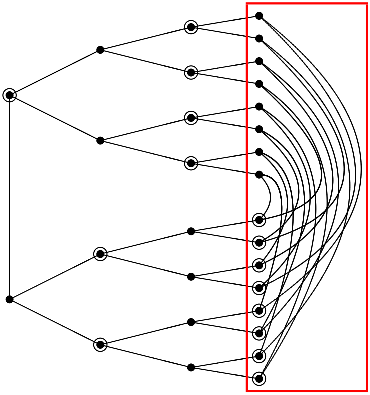
Question: Is $G_{\mathbb{F}}(xy, xy^2)$ the unique girth eight algebraically defined graph (up to isomorphism)?

- If so, we have an interesting characterization.
- If not, then we might be able to construct a new generalized quadrangle by replacing the boxed subgraph with this new girth eight graph. This is interesting because for a given odd prime power, only one GQ is known (up to isomorphism). Also, in the even order case, additional GQs can be constructed in this way.



Question: Is $G_{\mathbb{F}}(xy, xy^2)$ the unique girth eight algebraically defined graph (up to isomorphism)?

- If so, we have an interesting characterization.
- If not, then we might be able to construct a new generalized quadrangle by replacing the boxed subgraph with this new girth eight graph. This is interesting because for a given odd prime power, only one GQ is known (up to isomorphism). Also, in the even order case, additional GQs can be constructed in this way.



Conjecture (V. Dmytrenko, F. Lazebnik, J. Williford; 2007)

$G_{\mathbb{F}}(xy, xy^2)$ is the unique girth eight algebraically defined graph (up to isomorphism)

Connection to permutation polynomials

Theorem (V. Dmytrenko, F. Lazebnik, J. Williford; 2007)

Let $q = p^e$ be an odd prime power. Then every monomial graph of girth at least eight is isomorphic to the graph $G_q(xy, x^k y^{2k})$, where k is not divisible by p. If $q \geq 5$, then:

1. $((x+1)^{2k} - 1)x^{q-1-k} - 2x^{q-1} \in \mathbb{F}_q[x]$ *is a permutation polynomial of* $\mathbb{F}_q$.
2. $((x+1)^k - x^k)x^k \in \mathbb{F}_q[x]$ *is a permutation polynomial of* $\mathbb{F}_q$.

Connection to permutation polynomials

Theorem (V. Dmytrenko, F. Lazebnik, J. Williford; 2007)

Let $q = p^e$ be an odd prime power. Then every monomial graph of girth at least eight is isomorphic to the graph $G_q(xy, x^k y^{2k})$, where k is not divisible by p. If $q \geq 5$, then:

1. $((x+1)^{2k} - 1)x^{q-1-k} - 2x^{q-1} \in \mathbb{F}_q[x]$ *is a permutation polynomial of* $\mathbb{F}_q$.
2. $((x+1)^k - x^k)x^k \in \mathbb{F}_q[x]$ *is a permutation polynomial of* $\mathbb{F}_q$.

Theorem (Hermite-Dickson criterion)

Let $\mathbb{F}_q$ be of characteristic p. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:

1. f *has exactly one root in* $\mathbb{F}_q$.
2. *for each integer t with $1 \leq t \leq q-2$ and $p \nmid t$, the reduction of f^t* $\pmod{x^q - x}$ *has degree at most $q-2$.*

A Key Result

Theorem (V. Dmytrenko, F. Lazebnik, J. Williford; 2007)

Let $q = p^e$ be an odd prime power, with $e = 2^a 3^b$ for integers $a, b \geq 0$ and $p \geq 5$.
Then every girth eight monomial graph $G_q(x^u y^v, x^k y^m)$ is isomorphic to $G_q(xy, xy^2)$.

A Key Result

Theorem (V. Dmytrenko, F. Lazebnik, J. Williford; 2007)

Let $q = p^e$ be an odd prime power, with $e = 2^a 3^b$ for integers $a, b \geq 0$ and $p \geq 5$.
Then every girth eight monomial graph $G_q(x^u y^v, x^k y^m)$ is isomorphic to $G_q(xy, xy^2)$.

- This implies that for any q of this form, $G_q(xy, xy^2)$ is the girth eight unique monomial graph (up to isomorphism).

A Key Result

Theorem (V. Dmytrenko, F. Lazebnik, J. Williford; 2007)

Let $q = p^e$ be an odd prime power, with $e = 2^a 3^b$ for integers $a, b \geq 0$ and $p \geq 5$.
Then every girth eight monomial graph $G_q(x^u y^v, x^k y^m)$ is isomorphic to $G_q(xy, xy^2)$.

- This implies that for any q of this form, $G_q(xy, xy^2)$ is the girth eight unique monomial graph (up to isomorphism).
- What about q of other forms?

Additional Results

Theorem (BGK, 2012)

Let $q = p^e$ be an odd prime power, with $p \geq p_0$, a lower bound that depends only on the largest prime divisor of e.
Then every girth eight monomial graph $G_q(x^u y^v, x^k y^m)$ is isomorphic to $G_q(xy, xy^2)$.

Additional Results

Theorem (BGK, 2012)

Let $q = p^e$ be an odd prime power, with $p \geq p_0$, a lower bound that depends only on the largest prime divisor of e.
Then every girth eight monomial graph $G_q(x^u y^v, x^k y^m)$ is isomorphic to $G_q(xy, xy^2)$.

Example (What is p_0?)

- If $e = 2^a 3^b 5^c$ for integers $a, b, c \geq 0$, then $p \geq p_0 = 7$
- If $e = 2^a 3^b 5^c 7^d$ for integers $a, b, c, d \geq 0$, then $p \geq p_0 = 11$.
- If $e = 2^a 3^b 5^c 7^d 11^y$ for integers $a, b, c, d, y \geq 0$, then $p \geq p_0 = 13$.

Additional Results

Theorem (BGK, 2012)

Let $q = p^e$ be an odd prime power, with $p \geq p_0$, a lower bound that depends only on the largest prime divisor of e.
Then every girth eight monomial graph $G_q(x^u y^v, x^k y^m)$ is isomorphic to $G_q(xy, xy^2)$.

Example (What is p_0?)

- If $e = 2^a 3^b 5^c$ for integers $a, b, c \geq 0$, then $p \geq p_0 = 7$
- If $e = 2^a 3^b 5^c 7^d$ for integers $a, b, c, d \geq 0$, then $p \geq p_0 = 11$.
- If $e = 2^a 3^b 5^c 7^d 11^y$ for integers $a, b, c, d, y \geq 0$, then $p \geq p_0 = 13$.

This implies that for any q of this form, $G_q(xy, xy^2)$ is the unique girth eight monomial graph (up to isomorphism).

Breaking News!

Theorem (Hou, Lappano, Lazebnik, posted on ArXiv a few days ago)

Let q be an odd prime power. Then every girth eight monomial graph $G_q(x^u y^v, x^k y^m)$ is isomorphic to $G_q(xy, xy^2)$.

Can we say more over a different field?

Theorem (F. Lazebnik, J. Williford, and BGK)

Every girth eight polynomial graph $G_{\mathbb{C}}(x^k y^m, f)$, where $f \in \mathbb{C}[x, y]$, is isomorphic to $G_{\mathbb{C}}(xy, xy^2)$.

Can we say more over a different field?

Theorem (F. Lazebnik, J. Williford, and BGK)

Every girth eight polynomial graph $G_{\mathbb{C}}(x^k y^m, f)$*, where* $f \in \mathbb{C}[x, y]$*, is isomorphic to* $G_{\mathbb{C}}(xy, xy^2)$*.*

Note that f in the above theorem does not need to be a monomial; the result holds for any polynomial.

Connection back to the finite field case

Theorem (Lefschetz Principle)

Let ϕ be a sentence in the language of rings. The following are equivalent.

1. ϕ *is true in the complex numbers.*
2. ϕ *is true in every algebraically closed field of characteristic zero.*
3. ϕ *is true in some algebraically closed field of characteristic zero.*
4. *There are arbitrarily large primes p such that ϕ is true in some algebraically closed field of characteristic p.*
5. *There is an m such that for all $p > m$, ϕ is true in all algebraically closed fields of characteristic p.*

Connection back to the finite field case

Theorem (Lefschetz Principle)

Let ϕ be a sentence in the language of rings. The following are equivalent.

1. *ϕ is true in the complex numbers.*
2. *ϕ is true in every algebraically closed field of characteristic zero.*
3. *ϕ is true in some algebraically closed field of characteristic zero.*
4. *There are arbitrarily large primes p such that ϕ is true in some algebraically closed field of characteristic p.*
5. *There is an m such that for all $p > m$, ϕ is true in all algebraically closed fields of characteristic p.*

Informally, if $G_{\mathbb{C}}(x^k y^m, f)$ is not a candidate to replace $G_{\mathbb{C}}(xy, xy^2)$, then $G_q(x^k y^m, \hat{f})$ is not a candidate to replace $G_q(xy, xy^2)$ for "many" q.

Future Work

Open Problem

Do there exist f *and* g *in* $\mathbb{C}[x, y]$ *such that* $G = G_{\mathbb{C}}(f, g)$ *has girth eight and* G *is not isomorphic to* $G_{\mathbb{C}}(xy, xy^2)$*?*

Future Work

Open Problem

Do there exist f and g in $\mathbb{C}[x, y]$ such that $G = G_{\mathbb{C}}(f, g)$ has girth eight and G is not isomorphic to $G_{\mathbb{C}}(xy, xy^2)$?

1. This is done when g is a monomial (i.e. when $g = \alpha x^k y^m$ for $\alpha \in \mathbb{C}$).

Future Work

Open Problem

Do there exist f and g in $\mathbb{C}[x,y]$ such that $G = G_{\mathbb{C}}(f,g)$ has girth eight and G is not isomorphic to $G_{\mathbb{C}}(xy, xy^2)$?

1. This is done when g is a monomial (i.e. when $g = \alpha x^k y^m$ for $\alpha \in \mathbb{C}$).
2. G has a 4-cycle if and only if there exists a solution a, b, x, y to the system
$$\begin{cases} f(a,x) - f(b,x) + f(b,y) - f(a,y) = 0 \\ g(a,x) - g(b,x) + g(b,y) - g(a,y) = 0 \\ a \neq b, \;\; x \neq y. \end{cases}$$

Future Work

Open Problem

Do there exist f and g in $\mathbb{C}[x, y]$ such that $G = G_{\mathbb{C}}(f, g)$ has girth eight and G is not isomorphic to $G_{\mathbb{C}}(xy, xy^2)$?

1. This is done when g is a monomial (i.e. when $g = \alpha x^k y^m$ for $\alpha \in \mathbb{C}$).
2. G has a 4-cycle if and only if there exists a solution a, b, x, y to the system
$$\begin{cases} f(a,x) - f(b,x) + f(b,y) - f(a,y) = 0 \\ g(a,x) - g(b,x) + g(b,y) - g(a,y) = 0 \\ a \neq b, \;\; x \neq y. \end{cases}$$
3. G has a 6-cycle if and only if there exists a solution a, b, c, x, y, z to the system
$$\begin{cases} f(a,x) - f(b,x) + f(b,y) - f(c,y) + f(c,z) - f(a,z) = 0 \\ g(a,x) - g(b,x) + g(b,y) - g(c,y) + g(c,z) - g(a,z) = 0 \\ a \neq b, \;\; b \neq c, \;\; a \neq c; \;\; x \neq y, \;\; y \neq z, \;\; x \neq z. \end{cases}$$