On monomial graphs of girth eight: Some Corrections, Comments, and Clarifications

Brian Kronenthal

October 2, 2010

The following corrections and comments resulted from questions that arose while carefully reading [1], as well as discussions with Felix Lazebnik in an attempt to answer these questions. I have also corrected several typographical errors. This document was written with the purpose of clarifying certain elements of the paper.

- Page 3: Correct "Thge" to "The"
- Page 4: While Theorem 3 is correct as stated, the proof is much more clear with the following formulation:

  Theorem 3. *Let $q = p^e$ be an odd prime power, with $p \geq 5$ and $e = 2^a 3^b$ for integers $a, b \geq 0$.*

  1. *If $G_q(xy, x^k y^{2k})$ has girth at least eight and $p \nmid k$, then $k \equiv 1$ mod $(q-1)$. Furthermore, $1 \leq k < q$ (by Therorem 1a) implies $k = 1$.*
  2. *Every monomial graph of girth at least eight is isomorphic to Γ_3, and hence is of girth eight.*
  3. *For all q, $4 \leq q \leq 10^{10}$, every monomial graph nonisomorphic to Γ_3 has girth at most six.*

  To see the value of this formulation, consider the proof of Theorem 3 on page 13. In particular, note that the sentence "Using the induction hypothesis, we must have $k \equiv 1$ mod $(p^t - 1)$" follows much more clearly using the above statement.

- Page 6: The last two lines of the system of equations should be corrected as follows:

$$l_j^k = \sum_{i=1}^{k} f_j(p_1^i, l_1^i) - \sum_{i=1}^{k-1} f_j(p_1^{i+1}, l_1^i) - p_j^1,$$
$$p_j^1 = f_j(p_1^1, l_1^k) + \sum_{i=1}^{k-1} f_j(p_1^{i+1}, l_1^i) - \sum_{i=1}^{k} f_j(p_1^i, l_1^i) + p_j^1$$

- Page 7: Proposition 7a should read:

  "The degree of a nonlinear permutation polynomial does not divide $q - 1$...."

- Page 7: In the proof of Lemma 10, the third sentence of the second paragraph should read as follows:

  "Then the polynomial $f(x) = 1 + x + \ldots + x^t + (\beta - t - 1) \times (1 - (x-1)^{q-1}$ is a permutation polynomial since $f(x) = \phi_t(x)$ for all $x \neq 1$ and ...."

- Page 11: The proof of Lemma 15a is more clearly written as follows:

  Suppose to the contrary that $f(x) = \frac{x^{2k}-1}{(x-1)^k}$ is *not* one-to-one on $\mathbb{F}_q \setminus \{1\}$. Then there exist distinct $c, d \in \mathbb{F}_q \setminus \{1\}$ such that $f(c) = f(d)$.

  If (by way of contradiction and without loss of generality) $c = -1$, then

$$\frac{d^{2k}-1}{(d-1)^k} = f(d) = f(c) = f(-1) = \frac{(-1)^{2k}-1}{(-2)^k} = 0,$$

  which implies that $d^{2k} = 1$. Since $\gcd(2k, q-1) = 2$, $d^{2k} = 1$ implies[1] $d = \pm 1$. However, $d \in \mathbb{F}_q \setminus \{1\}$ forces $c = d = -1$, contradicting the distinctness of c and d. We thus conclude that $c \neq -1$ and $d \neq -1$. But this means $c, d \notin \{-1, 1\}$; therefore, $c^{2k}-1 \neq 0$ and $d^{2k}-1 \neq 0$.

- Page 11: The proof of Lemma 15b suggests using the same cycle S as in part a. However, the written cycle is not the same. Indeed, $S = (a, 0, 1; c, d, 1)$ should be used again.

- Page 13: In the proof of Theorem 3, change the second half of the first offset equation as follows:

$$\text{... and } 1 \leq k_0 + .. + k_N \leq \frac{p-1}{4}(N+1) \leq p-1$$

- Page 13: In the proof of Theorem 3, change the sentence under the first offset equation as follows:

  "Having $1 \leq \sum_{i=0}^{N} k_i \leq p-1$ and $k \equiv 1 \bmod (p-1)$, we conclude that $\sum_{i=0}^{N} k_i = 1$. Thus, $k_i \in \{0, 1\}$ and $p \nmid k$. We therefore conclude that $k_0 = 1$ and $k_1 = k_2 = ... = k_N = 0$; so $k = 1$."

- The paper implies that any monomial graph $G = G_q(xy, x^k y^{2k})$ with $k = p^a$, for some non-negative integer a, is isomorphic to Γ_3. To see this, consider the following isomorphism for mapping points and lines, respectively:

$$\Gamma_3 \to G_q(xy, x^{p^a} y^{2p^a}) \text{ such that } (p_1, p_2, p_3) \mapsto \left(p_1, p_2, p_3^{p^a}\right) \text{ and } [l_1, l_2, l_3] \mapsto \left[l_1, l_2, l_3^{p^a}\right] \qquad (*)$$

- Page 13 (bottom): Here is an explanation of the comment "It should be noted that this implies but is not equivalent to Conjecture 4..." We first summarize the two conjectures:

  Conjecture 4. *Any monomial graph $G_q(xy, x^k y^{2k})$ of girth eight is isomorphic to Γ_3.*

  Conjecture 16. *Let q be an odd prime power, $1 \leq k \leq q-1$, and $p \nmid k$. Then the polynomial $F(x)$ (and thus $H(x)$) is a permutation polynomial on $\mathbb{F}_q$ if and only if $k = 1$.*

  To prove the strength of Conjecture 16 relative to Conjecture 4, we first assume Conjecture 16 to be true. Then either $k = p^a$ and $F(x)$ is a permutation polynomial, or $k \neq p^a$ and $F(x)$ is not a permutation polynomial. In the first case, $k = p^a$ means that Conjecture 4 follows from the isomorphism (*). In the second case, the fact that $F(x)$ is not a permutation polynomial means that $G_q(xy, x^k y^{2k})$ contains a 6-cycle; so Conjecture 4 holds vacuously.

  Conversely, assume that Conjecture 4 holds; we will illustrate why Conjecture 16 does NOT immediately follow. When $k = p^a$, we know $F(x)$ must be a permutation polynomial (simply substitute $k = p^a$ in $F(x)$ and simplify in characteristic p). But when $F(x)$ is a permutation polynomial, it is not at all clear why Conjecture 4 must imply that $k = p^a$.

References

[1] V.Dmytrenko et al., On monomial graphs of girth eight, Finite Fields and Their Applications (2006).

[1] $d^{2k} = 1 \Rightarrow (d^2)^k = 1 \Rightarrow d^2 = 1$ because $\gcd(k, q-1) = 1$ implies that $x^k = 1$ has the unique solution $x = 1$. Thus, $d = \pm 1$.