Regular Maps of Given Face, Vertex and Petrie Orders in Fractional Linear Groups

J. Fraser

November 15, 2018

Abstract

We denote by (k, l, m)-regular map a regular map with face length k, vertex order l and Petrie walk length m. There is a conjecture that for all but finitely many triples k, l, m such that each pair is hyperbolic there exists a (k, l, m)-regular map. In this paper, we provide partial progress towards resolving this question. We shall show that for fixed hyperbolic k, l and all but finitely many values of m there exists a (k, l, m)-regular map whose automorphism group is a fractional linear group. To do this we shall give conditions for the existence of (k, l, m)-regular maps over fractional linear groups in terms of the existence of particular elements in finite fields. Further, we shall consider the special case of p, q two fixed distinct prime numbers, and r an arbitrary third prime, and give stronger simpler conditions for the existence of a (p, q, r)-regular map over fractional linear groups.

1 Introduction

A *regular map* is a map on a two dimensional surface permitting the highest possible degree of symmetry. The Platonic solids give a familiar example. A complete definition and further background material can be found at [3]. We shall refer to a regular map with face length k, vertex order l and Petrie dual walk length m as a (k, l, m)-regular map. Further, we shall only consider finite regular maps in this paper.

If M is a (k, l, m)-regular map, then the dual of M is an (l, k, m)-regular map and the Petrie dual of M is an (m, l, k)-regular map, hence we may consider the parameters of a (k, l, m)-regular map in an arbitrary order when discussing existence problems.

A (k, l, m)-regular maps exists on a spherical, Euclidean or hyperbolic surface depending on whether $1/k+1/l$ is greater than, equal to or less than $1/2$ respectively. In this paper, we provide a partial resolution to the conjecture that for all triples of parameters k, l, m, apart from finitely many exceptions, where each pair of parameters is hyperbolic, there exists a (k, l, m)-regular map. The method we apply is to attempt direct construction of (k, l, m)-regular maps in fractional linear groups. To do this, we make use of the classification of regular maps in fractional linear groups which can be taken from [1].

We now give some notation and definitions which we shall use throughout this paper:

- let $\varphi(n)$ be Euler's totient function;
- let $\Phi_n(x)$ be the n^{th} cyclotomic polynomial;
- let $\Psi_n(x)$ be the polynomial satisfying the equation $x^{\varphi(n)}\Psi_n(x + x^{-1}) = \Phi_n(x)$;
- let ξ_n denote a root of $\Phi_n(x)$;
- let ω_n denote a root of $\Psi_n(x)$, note we have $\omega_n = \xi_n + \xi_n^{-1}$ for some ξ_n;
- for a polynomial $f(x)$, let $\rho(f)$ denote the multiset of roots of $f(x)$ counted with multiplicity;
- we shall call a pair (k, l) *hyperbolic* if $1/k + 1/l < 1/2$, and we shall call a triple (k, l, m) hyperbolic if each pair $(k, l), (k, m), (l, m)$ is hyperbolic;

We shall begin with a section summarising the results of [1] which we shall use, as this will enormously aid the clarity of our exposition. The subsequent two sections will establish necessary and sufficient conditions respectively for the following theorem.

Proposition 1. *There exists a hyperbolic (k, l, m)-regular map in a fractional linear group over a finite field of characteristic p if, and only if, there is a solution to the equation*

$$\omega_k + \omega_l + \omega_m + 2 = 0$$

in a finite field of characteristic p where, for each $n \in \{k, l, m\}$, either $n = p$ or $p \nmid n$, and we do not have $(k, l, m) = (p, p, p)$.

In the case where k, l, m are three distinct primes p, q, r at least two of which are different, we are able to improve the previous condition to the following.

Proposition 2. *For a hyperbolic triple of primes p, q, r at least two of which are different, there exists a hyperbolic (p, q, r)-regular map whose automorphism group is isomorphic to a fractional linear group if, and only if, $N(p, q, r) > 1$, where $N(p, q, r) \in \mathbb{Z}$ is given by*

$$N(p, q, r) = \prod \omega_p + \omega_q + \omega_r + 2,$$

with the product being taken as ω_p, ω_q and ω_r are roots of $\Psi_p(x), \Psi_q(x)$ and $\Psi_r(x)$ respectively.

2 Summary of Regular Maps in Fractional Linear Groups

In the first half of this section, we assume that p is an odd prime and let K be an algebraically closed field of characteristic p. We first define the following matrices in $\mathrm{SL}(2, K)$ which we shall use throughout.

$$X_1 = \eta_1\beta_1 \begin{pmatrix} D_1 & \omega_{2l}\xi_{2k}D_1 \\ -\omega_{2l}\xi_{2k}^{-1} & -D_1 \end{pmatrix}, \qquad Y_1 = \beta_1 \begin{pmatrix} 0 & \xi_{2k}D_1 \\ \xi_{2k}^{-1} & 0 \end{pmatrix}, \qquad Z_1 = \beta_1 \begin{pmatrix} 0 & D_1 \\ 1 & 0 \end{pmatrix},$$

$$\text{where} \quad \eta_1 = (\xi_{2k} - \xi_{2k})^{-1}, \qquad \beta_1 = -1/\sqrt{-D_1}, \qquad D_1 = \omega_{2k}^2 + \omega_{2l}^2 - 4.$$

$$X_2 = \beta_2 \begin{pmatrix} 0 & \omega_{2l}^2 \\ 1 & 0 \end{pmatrix}, \qquad Y_2 = \eta_2\beta_2 \begin{pmatrix} \omega_{2l}^2 & 2\omega_{2l}^2 \\ -2 & -\omega_{2l}^2 \end{pmatrix}, \qquad Z_2 = \beta_2 \begin{pmatrix} 0 & \xi_{2l}\omega_{2l}^2 \\ \xi_{2l}^{-1} & 0 \end{pmatrix},$$

$$\text{where} \quad \eta_2 = (\xi_{2l} - \xi_{2l}^{-1})^{-1}, \qquad \beta_2 = -1/\sqrt{-D_2} \qquad D_2 = \omega_{2l}^2.$$

$$X_3 = \alpha \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \qquad Y_3 = \alpha \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \qquad Z_3 = \alpha \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$$\text{where} \quad \alpha^2 = -1.$$

Further, we define the groups $G_n \leq \mathrm{SL}(2, K)$ and their projections $\overline{G}_n \leq \mathrm{PSL}(2, K)$ as follows.

$$G_1(\xi_{2k}, \xi_{2l}) = \langle X_1, Y_1, Z_1 \rangle, \qquad \overline{G}_1(\xi_{2k}, \xi_{2l}) = \langle \overline{X}_1, \overline{Y}_1, \overline{Z}_1 \rangle,$$
$$G_2(\xi_{2l}) = \langle X_2, Y_2, Z_2 \rangle, \qquad \overline{G}_2(\xi_{2l}) = \langle \overline{X}_2, \overline{Y}_2, \overline{Z}_2 \rangle,$$
$$G_3 = \langle X_3, Y_3, Z_3 \rangle, \qquad \overline{G}_3 = \langle \overline{X}_3, \overline{Y}_3, \overline{Z}_3 \rangle.$$

Likewise, the regular map generated by $\overline{G}_1(\xi_{2k}, \xi_{2l})$ shall be called $M_1(\xi_{2k}, \xi_{2l})$ etc. We now state the key results we shall use.

Theorem 1 (Conder, Potočnik, Širáň)**.** *A hyperbolic (k, l)-regular map M has automorphism group a fractional linear group over a field of characteristic p if, and only if, one of the following cases occurs*

Case (i) $p \nmid k, l$ and there are some ξ_{2k}, ξ_{2l} such that $D_1 \neq 0$ and $M \cong M_1(\xi_{2k}, \xi_{2l})$;

Case (ii) $k = p \nmid l$ *and there is some* ξ_{2l} *such that* $D_2 \neq 0$ *and* $M \cong M_2(\xi_{2l})$*;*

Case (iii) $k = l = p$ *and* $M \cong M_3$*.*

We now give the corresponding theorem for the case of $p = 2$. As no hyperbolic pairs k, l have $k = 2$ or $l = 2$, we only have to consider one case when $p = 2$. Hence, we define the following matrices.

$$X_4 = \eta_4\beta_4 \begin{pmatrix} D_4 & \omega_l\xi_k D_4 \\ \omega_l\xi_k^{-1} & D_4 \end{pmatrix}, \qquad Y_4 = \beta_4 \begin{pmatrix} 0 & \xi_k D_4 \\ \xi_k^{-1} & 0 \end{pmatrix}, \qquad Z_4 = \beta_4 \begin{pmatrix} 0 & D_4 \\ 1 & 0 \end{pmatrix},$$
$$\text{where} \quad \eta_4 = (\xi_k + \xi_k^{-1})^{-1}, \qquad \beta_4 = 1/\sqrt{D_4}, \qquad D_4 = \omega_k^2 + \omega_l^2.$$

Further we define the corresponding $G_4(\xi_k, \xi_l)$ and $M_4(\xi_k, \xi_l)$. In this case we have $\mathrm{PSL}(2, K) \cong \mathrm{SL}(2, K)$, hence do not define $\overline{G}_4$. We now have the corresponding theorem.

Theorem 2. *A hyperbolic* (k, l)*-regular map* M *has automorphism group a fractional linear group of character 2 if, and only if,* $2 \nmid k, l$ *and there exist some* ξ_k, ξ_l *such that* $D_4(\xi_k, \xi_l) \neq 0$ *and* $M \cong M_4(\xi_k, \xi_l)$*.*

3 Equivalence

We begin with some lemmas. In the following, for any n and ξ_n, ξ_{2n}, we require the relationship $\xi_n = \xi_{2n}^2$ to hold. If we fix some ξ_{2n} then simply defining $\xi_n = \xi_{2n}^2$ gives the required relationship. However, if instead we fix some ξ_n we must show that there exists a choice of ξ_{2n} meeting the required relationship.

Lemma 1. *For any* n*, if* ξ_n *is a primitive root of order* n*, there exists a* ξ_{2n} *such that* $\xi_{2n}^2 = \xi_n$*.*

Proof. Let $\alpha, -\alpha$ be the solutions of $x^2 = \xi_n$ in K. From $\alpha^{2n} = \xi_n^n = 1$ we have $\mathrm{ord}(\alpha) \mid 2n$. If $\mathrm{ord}(\alpha) = m$, then $1 = \alpha^{2m} = \xi_n^m$ and $n \mid \mathrm{ord}(\alpha) \mid 2n$, hence $\mathrm{ord}(\alpha)$ is n or $2n$. We now consider the two cases of whether $\mathrm{ord}(\alpha)$ is even or odd. If $\mathrm{ord}(\alpha) = 2m$ is even, then $1 = \alpha^{2m} = \xi_n^m$, and so $m = n$ and we may take $\xi_{2n} = \alpha$. If $\mathrm{ord}(\alpha) = m$ is odd, then $\mathrm{ord}(-\alpha) = 2m$ is even and we may take $\xi_{2n} = -\alpha$. □

Lemma 2. *In* K *we have* $\omega_p = 2$ *and* $\omega_{2p} = -2$*.*

Proof. In our notation, ω_n is defined to be a fixed root of $\Psi_n(x)$. Hence we show $\Psi_p(x) = (x-2)^{(p-1)/2}$ and $\Psi_{2p} = (x+2)^{(p-1)/2}$ in K. This is a simple consequence of the fact $\Phi_p(x) = (x-1)^{p-1}$ and $\Phi_{2p} = (x+1)^{p-1}$ in K, and the identity $x^{\varphi(n)}\Psi_n(x + x^{-1}) = \Phi_n(x)$. □

Lemma 3. *For any* $\overline{X} \in \mathrm{PSL}(2, K)$ *with pre-image* $X \in \mathrm{SL}(2, K)$*, we have* $\mathrm{ord}(\overline{X}) = n$ *if, and only if,* $\mathrm{tr}(X)^2 = \omega_{2n}^2$ *for some element* $\omega_{2n} \in K$*.*

Proof. We shall consider separately the cases $p \mid n$ and $p \nmid n$. For $p \nmid n$, first suppose that $\mathrm{ord}(\overline{X}) = n$ and X is a pre-image of $\overline{X}$. As X is a pre-image of $\overline{X}$, we have either $\mathrm{ord}(X) = n$ and n is odd or $\mathrm{ord}(X) = 2n$. If $\mathrm{ord}(X) = 2n$ then $\mathrm{tr}(X) = \omega_{2n}$ and we are done. If $\mathrm{ord}(X) = n$ then $\mathrm{tr}(X)^2 = \mathrm{tr}(-X)^2 = \omega_{2n}^2$ and we are done. Conversely, if $\mathrm{tr}(X)^2 = \omega_{2n}$, then without loss of generality we have $\mathrm{tr}(X) = \omega_{2n}$ and $\mathrm{tr}(-X) = -\omega_{2n}$. Hence, $\mathrm{ord}(X) = 2n$ and so $\mathrm{ord}(\overline{X}) = n$.

For $p \mid n$, first suppose that $\mathrm{ord}(\overline{X}) = p$ and that X is a pre-image of $\overline{X}$. As X is a pre-image of $\overline{X}$, we have either $\mathrm{ord}(X) = p$ or $\mathrm{ord}(X) = 2p$. In the first case, $\mathrm{tr}(X) = 2$ and in the second $\mathrm{tr}(X) = -2$. Hence, in either case, $\mathrm{tr}(X)^2 = 4 = \omega_{2p}^2$. Conversely, if $\mathrm{tr}(X)^2 = \omega_{2p}^2 = 4$ then $\mathrm{tr}(X) = 2$ or $\mathrm{tr}(X) = -2$, giving $\mathrm{ord}(X) = p$ or $\mathrm{ord}(X) = 2p$ respectively. In either case, $\mathrm{ord}(\overline{X}) = p$. □

Lemma 4. *For any finite field* K *of characteristic* p *and fixed* ω_k, ω_l*, there is a uniquely determined element* $\omega = \xi + \xi^{-1}$ *such that* $\omega_k + \omega_l + \omega + 2 = 0$*. Further, we can uniquely define a number* m *either by* $m = \mathrm{ord}(\xi) = \mathrm{ord}(\xi^{-1})$*, or if* $\xi = \xi^{-1} = 1$ *by* $m = p$*. In either case, we have that* ω *is a root of* $\Psi_m(x)$*.*

Proof. Let $\omega = -(\omega_k + \omega_l + 2)$. The equation $f(x) = x^2 - \omega x + 1 = 0$ has two uniquely determined roots. Let ξ be a root of $f(x)$, we see that ξ^{-1} is the other root of $f(x)$. If $\mathrm{ord}(\xi) \neq 1$ then we must have $p \nmid \mathrm{ord}(\xi)$ and letting $m = \mathrm{ord}(\xi)$ we have $\Phi_m(\xi) = 0$, hence $\Psi_m(\omega) = \Psi_m(\xi + \xi^{-1}) = \xi^{-\varphi(m)/2}\Phi_m(\xi) = 0$. In the case where $\mathrm{ord}(\xi) = 1$, then we have $\xi = \xi^{-1} = 1$ and $\omega = 2$. Hence, by Lemma 2 we have $\Psi_p(\omega) = 0$. □

Remark. *In subsequent work we now may refer to the element ω_m as the unique solution to the equation $\omega_k + \omega_l + \omega_m + 2 = 0$ for some fixed ω_k, ω_l; noting the technical difficulty in the case $m = p$ addressed in this lemma.*

Proposition 3. *For ξ_{2k}, ξ_{2l} such that $D_1(\xi_{2k}, \xi_{2l}) \neq 0$ the map $M_1(\xi_{2k}, \xi_{2l})$ is a (k, l, m)-regular map where m is defined by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$.*

Proof. From Theorem 1 we know that $M_1(\xi_{2k}, \xi_{2l})$ is a (k, l)-regular map. Therefore, we simply calculate the Petrie dual order of $M_1(\xi_{2k}, \xi_{2l})$. The Petrie dual order of $M_1(\xi_{2k}, \xi_{2l})$ is the order of the element $\overline{Z}_1\overline{X}_1\overline{Y}_1$ in $\overline{G}_1$. We may apply Lemma 3 and we calculate $\mathrm{ord}(\overline{Z}_1\overline{X}_1\overline{Y}_1) = m$ where $\mathrm{tr}(Z_1X_1Y_1)^2 = \omega_{2m}^2$. We calculate $Z_1X_1Y_1$ as follows.

$$\begin{aligned} Z_1X_1Y_1 &= \eta_1\beta_1^3 \begin{pmatrix} 0 & D_1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} D_1 & \omega_{2l}\xi_{2l}D_1 \\ \omega_{2l}\xi_{2l}^{-1} & -D_1 \end{pmatrix} \begin{pmatrix} 0 & \xi_{2k}D_1 \\ \xi_{2k}^{-1} & 0 \end{pmatrix} \\ &= -\eta_1\beta_1 \begin{pmatrix} \omega_{2l}\xi_{2l}^{-1} & -D_1 \\ 1 & \omega_{2l}\xi_{2l} \end{pmatrix} \begin{pmatrix} 0 & \xi_{2k}D_1 \\ \xi_{2k}^{-1} & 0 \end{pmatrix} = -\eta_1\beta_1 \begin{pmatrix} -\xi_{2k}^{-1}D_1 & \omega_{2l}D_1 \\ \omega_{2l} & \xi_{2k}D_1 \end{pmatrix}. \end{aligned}$$

This gives us $\mathrm{tr}(Z_1X_1Y_1) = -\eta_1\beta_1(\xi_{2k} - \xi_{2k}^{-1})D_1 = -D_1/\sqrt{-D_1}$. Therefore $\omega_{2m}^2 = -D_1 = 4 - \omega_{2k}^2 - \omega_{2l}^2$, and so $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$. Hence ω_m is the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$. □

Proposition 4. *For ξ_{2l} such that $D_2(\xi_{2l}) \neq 0$ the map $M_2(\xi_{2l})$ is a (k, l, m)-regular map where $k = p, \omega_k = \omega_p$ and m is defined by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$.*

Proof. We proceed as in the previous proposition. We calculate $\omega_{2m}^2 = \mathrm{tr}(Z_2X_2Y_2)^2$ as follows.

$$\begin{aligned} Z_2X_2Y_2 &= \eta_2\beta_2^3 \begin{pmatrix} 0 & \xi_{2l}\omega_{2l}^2 \\ \xi_{2l}^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & \omega_{2l}^2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \omega_{2l}^2 & 2\omega_{2l}^2 \\ -2 & -\omega_{2l}^2 \end{pmatrix} \\ &= -\eta_2\beta_2 \begin{pmatrix} \xi_{2l} & 0 \\ 0 & \xi_{2l}^{-1} \end{pmatrix} \begin{pmatrix} \omega_{2l}^2 & 2\omega_{2l}^2 \\ -2 & -\omega_{2l}^2 \end{pmatrix} = -\eta_2\beta_2 \begin{pmatrix} \xi_{2l}\omega_{2l}^2 & 2\xi_{2l}\omega_{2l}^2 \\ -2\xi_{2l}^{-1} & -\xi_{2l}^{-1}\omega_{2l}^2 \end{pmatrix}. \end{aligned}$$

This gives $\mathrm{tr}(Z_2X_2Y_2) = -\eta_2\beta_2(\xi_{2l} - \xi_{2l}^{-1})\omega_{2l}^2 = \omega_{2l}^2/\sqrt{-\omega_{2l}^2}$. Hence $\omega_{2m}^2 = \mathrm{tr}(Z_2X_2Y_2)^2 = -\omega_{2l}^2$. This gives $\omega_{2l}^2 + \omega_{2m}^2 = 0$. As $k = p$ we have $\omega_{2k}^2 = 4$, giving $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$, and so ω_m is the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$. □

Proposition 5. *The map M_3 is a (k, l, m)-regular map where $k = l = p, \omega_k = \omega_l = \omega_p$ and m is defined by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$.*

Proof. We calculate $\omega_{2m}^2 = \mathrm{tr}(Z_3X_3Y_3)^2$ as follows.

$$Z_3X_3Y_3 = \alpha^3 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = -\alpha \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = -\alpha \begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}.$$

This gives $\mathrm{tr}(Z_3X_3Y_3) = -2\alpha$ and hence $\mathrm{tr}(Z_3X_3Y_3)^2 = -4$. Therefore, as $\omega_{2k}^2 = \omega_{2l}^2 = 4$ we have $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$, and so ω_m is the unqiue solution to $\omega_k + \omega_l + \omega_m + 2 = 0$. □

We now deal with the case of $p = 2$.

Proposition 6. *For ξ_k, ξ_l such that $D_4(\xi_k, \xi_l) \neq 0$ the map $M_4(\xi_k, \xi_l)$ is a (k, l, m)-regular map where m is defined by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$.*

Proof. Lemma 3 does not apply in this case. However, for any $2 \nmid n$ we have $\mathrm{ord}(M) = n$ if, and only if, $\mathrm{tr}(M) = \omega_n$ for $M \in \mathrm{SL}(2, K)$. Hence, we take $\omega_m = \mathrm{tr}(Z_4X_4Y_4)$ where m is the Petrie order of $M_4(\xi_k, \xi_l)$. We calculate $Z_4X_4Y_4$ as follows.

$$\begin{aligned} Z_4X_4Y_4 &= \eta_4\beta_4^3 \begin{pmatrix} 0 & D_4 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} D_4 & \omega_l\xi_kD_4 \\ \omega_l\xi_k^{-1} & D_4 \end{pmatrix} \begin{pmatrix} 0 & \xi_kD_4 \\ \xi_k^{-1} & 0 \end{pmatrix} \\ &= \eta_4\beta \begin{pmatrix} \omega_l\xi_k^{-1} & D_4 \\ 1 & \omega_l\xi_k \end{pmatrix} \begin{pmatrix} 0 & \xi_kD_4 \\ \xi_k^{-1} & 0 \end{pmatrix} = \eta_4\beta_4 \begin{pmatrix} \xi_k^{-1}D_4 & \omega_lD_4 \\ \omega_l & \xi_kD_4 \end{pmatrix}. \end{aligned}$$

Hence $\mathrm{tr}(Z_4X_4Y_4) = \eta_4\beta_4(\xi_k + \xi_k^{-1})D_4 = D_4/\sqrt{D_4}$. This gives $\omega_m^2 = D_4 = \omega_k^2 + \omega_l^2$, which is equivalent to $\omega_k^2 + \omega_l^2 + \omega_m^2 = 0$ and hence as squaring is the Frobenius automorphism in finite fields of characteristic 2 we have $\omega_k + \omega_l + \omega_m + 2 = 0$ as required. □

We now have the necessary groundwork to prove Proposition 1.

Proof. The combination of theorems 1 and 2 with propositions 3, 4, 5 and 6 tell us that if M is a hyperbolic (k, l)-regular map with automorphism group a fractional linear group over a field of characteristic p, then there is a solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ in a suitable extension of $\mathrm{GF}(p)$. Now, conversely, suppose that we have a solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ for some hyperbolic triple k, l, m in a finite field of characteristic p. If $p \neq 2$, we first define ξ_{2k}, ξ_{2l} and ξ_{2m} using Lemma 1. As k, l, m is hyperbolic, we have $\omega_{2m}^2 \neq \omega_4^2 = 0$. Hence we have $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$ and so $\omega_{2k}^2 + \omega_{2l}^2 - 4 = -\omega_{2m}^2 \neq 0$.

- Case (i) $p \neq 2$ and $p \nmid k, l$, in this case we have $D_1(\xi_{2k}, \xi_{2l}) = \omega_{2k}^2 + \omega_{2l}^2 - 4 \neq 0$, hence we may use Theorem 1 and Proposition 3 to show that $M_1(\xi_{2k}, \xi_{2l})$ is a (k, l, m)-regular map with automorphism group a fractional linear group.
- Case (ii) $p \neq 2$ and $p = k \nmid l$, in this case we have $D_2(\xi_{2l}) = \omega_{2l}^2 = \omega_{2k}^2 + \omega_{2l}^2 - 4 \neq 0$, hence we may use Theorem 1 and Proposition 4 to show that $M_2(\xi_{2l})$ is a (k, l, m)-regular map with automorphism group a fractional linear group.
- Case (iii) $p = k = l$, in this case we may use Theorem 1 and Proposition 5 to show that M_3 is a (k, l, m)-regular map with automorphism group a fractional linear group.

Finally, we deal with the case $p = 2$. In this case, the fact k, l, m is hyperbolic tells us that $p \nmid k, l, m$. As $2 \nmid k, l, m$, we must have $\omega_k, \omega_l, \omega_m \neq 0$. Hence applying the Frobenius automorphism to $\omega_k + \omega_l + \omega_m + 2 = 0$ we have $\omega_k^2 + \omega_l^2 = \omega_m^2 \neq 0$. Hence we have $D_4(\xi_k, \xi_l) = \omega_k^2 + \omega_l^2 \neq 0$ and we may apply Theorem 2 and Proposition 6 to show that $M_4(\xi_k, \xi_l)$ is a (k, l, m)-regular map with automorphism group a linear fractional group. □

4 Solving The Equation

For $p \nmid 2, k, l, m$ and K a finite field of characteristic p, we now have that a (k, l, m)-regular map exists with automorphism group $\mathrm{PSL}(2, K)$ or $\mathrm{PGL}(2, K)$ if, and only if, there exists a solution to the equation $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$ in a finite field of characteristic p. We now aim to prove the following proposition.

Proposition 7. *For fixed k, l, such that $1/k + 1/l > 1/2$, there are only finitely many values m such that there is no solution to $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$ in any finite field of characteristic $p \nmid 2, k, l, m$.*

Lemma 5. *The existence of solutions to the equation $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$ in a field of characteristic p is equivalent to the existence of solutions to the equation $\omega_k + \omega_l + \omega_m + 2 = 0$ in a field of characteristic p.*

Proof. We simply expand each $\omega_{2n}^2 = (\xi_{2n} + \xi_{2n}^{-1})^2 = \xi_{2n}^2 + 2 + \xi_{2n}^{-2}$ and note that ξ_{2n} is order $2n$ implies ξ_{2n}^2 is order n, allowing us to take $\xi_n = \xi_{2n}^2$. □

We now consider the functions $\Psi_n(x)$ of Lehmer [2] defined by the identity

$$x^{\varphi(n)}\Psi_n(x + x^{-1}) = \Phi_n(x),$$

where $\Phi_n(x)$ is the n^{th} cyclotomic polynomial. We extract the following construction of $\Psi_n(x)$ from [4]. We define the series of polynomials $C_n(x)$ by $C_1(x) = 1, C_2(x) = x + 2, C_3(x) = x + 1, C_4(x) = x^2 + 2x$ and $C_{n+2}(x) = xC_n(x) - C_{n-2}(x)$. Then the polynomial $\Psi_n(x)$ is given by the relation

$$\Psi_n(x) = C_n(x) \Bigg/ \left(\prod_{\substack{d|n \\ d \neq n}} \Psi_d(x) \right).$$

Though we shall not make direct use of this construction within this paper, the author has found it useful for computation with these polynomials. Further, we note that the roots of $\Psi_n(x)$ are exactly $\xi_n + \xi_n^{-1}$ where ξ_n is any n^{th} root of unity. We now define the $N(k,l,m) \in \mathbb{C}$ for each k,l,m as follows.

$$N(k,l,m) = \prod \omega_k + \omega_l + \omega_m + 2,$$

Where the product is taken with $\omega_k, \omega_l, \omega_m$ taking the values of all distinct triples of roots of Ψ_k, Ψ_l and Ψ_m respectively.

Lemma 6. *$N(k,l,m) \in \mathbb{Z}$.*

Proof. The number $N(k,l,m)$ is a symmetric function of the roots of polynomials over $\mathbb{Z}[x]$, and therefore an integer. □

Lemma 7. *There is solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ in a finite field of characteristic $p \nmid 2, k, l, m$ if, and only if, $p \mid N(k,l,m)$.*

Proof. As $N(k,l,m)$ is a symmetric function of the roots of polynomials over $\mathbb{Z}[x]$, it is mapped from $\mathbb{Z}$ to $\mathrm{GF}(p)$ by the natural homomorphism for all p. For a given value $p \nmid 2, k, l, m$, we may calculate $N(k,l,m)$ either via its image under the homomorphism or direct computation over the product as in the definition of $N(k,l,m)$. Therefore, $N(k,l,m) = 0$ in $\mathrm{GF}(p)$ if and only if one of the terms in the product for $N(k,l,m)$ is zero, which corresponds exactly to a solution of $\omega_k + \omega_l + \omega_m + 2 = 0$. Finally, $N(k,l,m) = 0$ in $\mathrm{GF}(p)$ is equivalent to $p \mid N(k,l,m)$. □

We now define the functions $f_{k,l}(x) \in \mathbb{Z}[x]$ and show that the condition $p \mid N(k,l,m)$ is equivalent to $f_{k,l}$ having a root of order m in some extension of $\mathrm{GF}(p)$. We define $f_{k,l}$ as follows.

$$f_{k,l}(x) = \prod x^2 + x(\omega_k + \omega_l + 2) + 1,$$

where the product is taken in $\mathbb{Q}(\omega_k, \omega_l)$ over all roots ω_k, ω_l of Ψ_k and Ψ_l respectively.

Lemma 8. *A prime $p \nmid 2, k, l, m$ is a divisor of $N(k,l,m)$ if, and only if, $f_{k,l}(x)$ has a root of order m in an extension of* $\mathrm{GF}(p)$.

Proof. Suppose that $N(k,l,m) = 0$ in $\mathrm{GF}(p)$, then in a suitable extension of $gf(p)$ we have

$$N(k,l,m) = \prod \omega_k + \omega_l + \omega_m + 2 = \prod \xi_m^{-1}(\xi_m^2 + \xi_m(\omega_k + \omega_l + 2) + 1) = \alpha \prod f_{k,l}(\xi_m),$$

where α is a product of some m^{th} roots of unity and therefore non-zero. Hence the product $\prod f_{k,l}(\xi_m)$ taken over half of the m^{th} roots of unity must have at least one term equal to zero, which is equivalent to $f_{k,l}(x)$ having a root of order m in an extension of $\mathrm{GF}(p)$. For the converse, suppose that ξ_m is a root of $f_{k,l}(x)$ in $\mathrm{GF}(p)$, then

$$0 = f_{k,l}(\xi_m) = \xi_m^2 + \xi_m(\omega_k + \omega_l + 2) + 1 = \xi_m^{-1}(\xi_m + \xi_m^{-1} + \omega_k + \omega_l + 2) = \omega_k + \omega_l + \omega_m + 2.$$

Hence we see in the product formula for $N(k,l,m)$ that $N(k,l,m) = 0$ in $\mathrm{GF}(p)$. □

Now we aim to show for each $f_{k,l}(x)$ that there are only finitely many numbers m such that $f_{k,l}(x)$ has no roots of order m in any finite field of characteristic $p \nmid 2, k, l, m$. To do this, we lift a result from [**?**] which states.

Theorem 3. *If a polynomial $f(x) \in \mathbb{Z}[x]$ has no repeated roots, and $x, \Phi_n \nmid f(x)$ for any n, then f takes roots of all but finitely many orders in finite fields.*

We now show that every $f_{k,l}$, with a few exceptions, must have at least one irreducible factor with these properties.

Lemma 9. *If k,l satisfy $1/k + 1/l < 1/2$, then $f_{k,l}$ has at least one factor $g_{k,l}(x) \in \mathbb{Z}[x]$ such that $x, \Phi_n \nmid g_{k,l}(x)$ for any value of n.*

Proof. We have

$$f_{k,l}(x) = \prod x^2 + x(\omega_k + \omega_l + 2) + 1,$$

where the product is taken over all roots of Ψ_k and Ψ_l. The expression $x^2 + Cx + 1$ has two real roots, neither of which have absolute value 1, provided $C^2 - 4 > 0$. Therefore, if there is some ω_k and ω_l such that $(\omega_k + \omega_l + 2)^2 > 4$, then $f_{k,l}(x)$ has real roots of absolute value not equal to zero, and hence has an irreducible factor not divisible by a cyclotomic polynomial.

For $n \geq 5$, taking $\xi = e^{i2\pi/n}$ we have that ξ is an n^{th} root of unity and that $\xi + \xi^{-1} = 2\cos(2\pi/n) > 0$. Hence, if $k, l \geq 5$ then we can find some $\omega_k, \omega_l > 0$ giving $(\omega_k + \omega_l + 2)^2 > 4$, as required.

For $k = 4$, we have $\omega_k = 0$, hence taking $l \geq 5$ we can find a pair of ω_k, ω_l such that $(\omega_k + \omega_l + 2)^2 > 4$.

For $k = 3$, we have $\omega_k = -1$, hence taking $l \geq 7$ and considering $\xi = e^{i2\pi/l}$ we have $\omega = 2\cos(2\pi/l) > 1$, giving us $(\omega_k + \omega_l + 2)^2 > 4$.

Hence, all parameters corresponding to $1/k + 1/l > 1/2$, i.e. all hyperbolic k and l, allow us to deduce the existence of our desired factor $g_{k,l}$. □

We now define $g_{k,l}(x)$ to be the largest factor of $f_{k,l}(x)$ such that $g_{k,l}(x)$ has no repeated roots, and $x, \Phi_n(x) \nmid g_{k,l}(x)$ for any n. We now state another corollary that may prove useful for computational purposes.

Corollary 1. *The Mahler measure of $g_{k,l}(x)$ is at least*

$$\cos(2\pi/k) + \cos(2\pi/l) + 1 + \sqrt{(\cos(2\pi/k) + \cos(2\pi/l) + 1)^2 - 1}.$$

Proof. Simply take the value of the larger root of $x^2 + x(\omega_k + \omega_l + 2) + 1$ when $\omega_k + \omega_l$ is at a maximum as the lower bound. □

We are now in a position to prove Proposition 7.

Proof. We use Theorem 3 of [?]. Theorem 3 shows the equivalence to roots of a polynomial f of order n, and *primitive prime divisors* in the sequence $a_n = \prod f(\xi)$, where ξ ranges over the roots of unity of order n. A divisor of a_n is primitive if $p \mid a_n$ but $p \nmid n$, and Theorem 3 tells us that for all $n > N$ each a_n has at least one primitive divisor. Further, we know that a given prime p can only appear as a primitive prime divisor of at most $\deg(f)$ elements a_n.

In our case, let $a_n = \prod g_{k,l}(\xi)$. The set of primes which divide $2, k$ or l is finite, and hence there is some N such that for any $n > N$ no prime divisor of $2, k$ or l can appear as a prime divisor of a_n. Therefore, there is an N' such that for any $n > N'$ all a_n have a primitive divisor other than a divisor of $2, k$ or l. For any particular $m > N'$, let p be a primitive prime divisor of a_m. Theorem 3 tells us that $g_{k,l}$ has a root of order m in a suitable extension field K of $\mathrm{GF}(p)$. Further, we know $p \nmid 2, k, l$ from our choice of N' and $p \nmid m$ as p is a primitive divisor. As $g_{k,l}(x)$ is a factor of $f_{k,l}(x)$ in $\mathbb{Z}[x]$, it is a factor of $f_{k,l}(x)$ in K also. Hence, $f_{k,l}(x)$ has a root of order m in an extension field of $\mathrm{GF}(p)$ where $p \nmid 2, k, l, m$, and by Lemma 8 we are done. □

5 The Case p, q, r Are Prime

In the case where p, q are two fixed distinct primes and r is an arbitrary third prime such that (p, q, r) is hyperbolic we are in a position to say more about the situation. We first wish to show that in the case of primes, the polynomial $f_{p,q}(x)$ is irreducible. To do this, first we need a lemma.

Lemma 10. $[\mathbb{Q}(\omega_p + \omega_q) : \mathbb{Q}] = (p-1)(q-1)/4$.

Proof. In the case $p = 3$ we have $\omega_p = 1$ and the result is trivial. Hence we assume that $p, q > 3$. To show the result, we shall use the following facts.

(i) if $L : K$ is a normal extension of K, and M is an intermediate field $K \subseteq M \subseteq L$, then $[L : M] = |\Gamma(L/M)|$;

(ii) the field extension $\mathbb{Q}(\xi_{pq}) : \mathbb{Q}$ is a normal extension and $[\mathbb{Q}(\xi_{pq}) : \mathbb{Q}] = (p-1)(q-1)$;

(iii) $\mathbb{Q}(\xi_p) \cap \mathbb{Q}(\xi_q) = \mathbb{Q}$.

Our strategy is to calculate $[\mathbb{Q}(\xi_{pq}):\mathbb{Q}(\omega_p+\omega_q)]$ by explicitly calculating $G=\Gamma(\mathbb{Q}(\xi_{pq})/\mathbb{Q}(\omega_p+\omega_q))$. We know that each automorphism $\phi \in H=\Gamma(\mathbb{Q}(\xi_{pq})/\mathbb{Q})$ is uniquely defined by some n coprime to pq and the fact for any pq^{th} root of unity ξ we have $\phi(\xi)=\xi^n$. From the Galois correspondence we know that $G \leq H$. If $\phi \in G$, then we must have $\phi(\omega_p+\omega_q)=\omega_p+\omega_q$, as G fixes $\mathbb{Q}(\omega_p+\omega_q)$, and further we know that if $\phi \in H$ and $\phi(\omega_p+\omega_q)=\omega_p+\omega_q$ then ϕ fixes $\mathbb{Q}(\omega_p+\omega_q)$. Therefore, $G=\{\phi \in H \mid \phi(\omega_p+\omega_q)=\omega_p+\omega_q\}$. We now find all such ϕ. Suppose $\phi \in H$ and $\phi(\omega_p+\omega_q)=\omega_p+\omega_q$. We may choose ξ_{pq} such that $\omega_p=\xi_{pq}^q+\xi_{pq}^{-q}$ and $\omega_q=\xi_{pq}^p+\xi_{pq}^{-p}$. Let n be the unique number $1 \leq n < pq$ such that $(n,pq)=1$ and $\phi(\xi_{pq})=\xi_{pq}^n$. This gives us

$$\begin{aligned}\xi_{pq}^q+\xi_{pq}^{-q}+\xi_{pq}^p+\xi_{pq}^{-p} &= \omega_p+\omega_q=\phi(\omega_p+\omega_q)=\phi(\xi_{pq}^q)+\phi(\xi_{pq}^{-q})+\phi(\xi_{pq}^p)+\phi(\xi_{pq}^{-p})\\ &= \xi_{pq}^{nq}+\xi_{pq}^{-nq}+\xi_{pq}^{np}+\xi_{pq}^{-np}.\end{aligned}$$

We may rearrange this equation to the following equivalent equation.

$$\xi_p+\xi_p^{-1}-\xi_p^n-\xi_p^{-n}=\xi_q+\xi_q^{-1}-\xi_q^n-\xi_q^{-n},$$

where $\xi_p=\xi_{pq}^q$ and $\xi_q=\xi_{pq}^p$. As the left hand side is in $\mathbb{Q}(\xi_p)$ and the right hand side is in $\mathbb{Q}(\xi_q)$, we must have that both are in $\mathbb{Q}(\xi_p)\cap\mathbb{Q}(\xi_q)=\mathbb{Q}$. As one of $p,q>5$, we may take $p>5$, hence we know that the p^{th} roots of unity form a set of more than four algebraic numbers linearly independent over $\mathbb{Q}$ and so a sum of at most 4 distinct p^{th} roots of unity equal to a number in $\mathbb{Q}$ must be a trivial sum and equal to zero. This gives us

$$\xi_p+\xi_p^{-1}=\xi_p^n+\xi_p^{-n} \quad \text{and} \quad \xi_q+\xi_q^{-1}=\xi_q^n+\xi_q^{-n}.$$

From the left hand side we get $n \equiv \pm 1 \pmod p$, and from the right we get $n \equiv \pm 1 \pmod q$. It is now trivial to show that this gives us exactly four distinct automorphisms. Therefore $|G|=4$, and we have

$$(p-1)(q-1)=[\mathbb{Q}(\xi_{pq}):\mathbb{Q}]=[\mathbb{Q}(\xi_{pq}):\mathbb{Q}(\omega_p+\omega_q)][\mathbb{Q}(\omega_p+\omega_q):\mathbb{Q}]=4[\mathbb{Q}(\omega_p+\omega_q):\mathbb{Q}],$$

i.e. $[\mathbb{Q}(\omega_p+\omega_q):\mathbb{Q}]=(p-1)(q-1)/4$, as desired. □

Proposition 8. *The polynomial $f_{p,q}(x)$ is irreducible.*

Proof. Let α be a root of a factor $x^2+(\omega_p+\omega_q+2)x+1$ of $f_{p,q}(x)$ for $\omega_p+\omega_q<0$. We consider $[\mathbb{Q}(\alpha):\mathbb{Q}]$. First, we have that $\deg(f_{p,q}(x))=(p-1)(q-1)/2$, and hence $[\mathbb{Q}(\alpha):\mathbb{Q}]=(p-1)(q-1)/2$ if, and only if, $f_{p,q}(x)$ is irreducible. We have that $\alpha+\alpha^{-1}=-(\omega_p+\omega_q+2)$, giving $\mathbb{Q}(\omega_p+\omega_q)\subseteq\mathbb{Q}(\alpha)$. Further, as we chose $\omega_p+\omega_q<0$, we must have $\alpha \in \mathbb{C}$, and $\mathbb{Q}(\alpha)\neq\mathbb{Q}(\omega_p+\omega_q)$. Hence, as $g(x)=x^2+(\omega_p+\omega_q+2)x+1 \in \mathbb{Q}(\omega_p+\omega_q)$, we must have $[\mathbb{Q}(\alpha):\mathbb{Q}(\omega_p+\omega_q)]=2$, and so $[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\omega_p+\omega_q)][\mathbb{Q}(\omega_p+\omega_q):\mathbb{Q}]=(p-1)(q-1)/2$, showing $f_{p,q}(x)$ is irreducible. □

Corollary 2. *No cyclotomic polynomial $\Phi_n(x) \mid f_{p,q}(x)$.*

Proof. From Lemma 9 we know that $f_{p,q}(x)$ is an irreducible polynomial with at least one root of absolute value greater than 1. □

Lemma 11. *The number $N(p,q,r)>0$.*

Proof. □

Proposition 9. *There is a hyperbolic (p,q,r)-regular map in fractional linear groups if, and only if, $N(p,q,r)>1$.*

Proof. □

References

[1] Marston Conder, Primož Potočnik, and Jozef Širáň. Regular hypermaps over projective linear groups. *Journal of the Australian Mathematical Society*, pages 155–175, 2008.

[2] D. H. Lehmer. A note on trigonometric algebraic numbers. *The American Mathematical Monthly*, pages 165–166, 1933.

[3] Jozef Širáň. How symmetric can maps on surfaces be? *Surveys in Combinatorics*, 2013.

[4] Steve Wilson. Applications and refinements of vince's construction. *Geometriae Dedicata*, pages 231–242, 1993.