Glasgow Math. J. **53** (2011) 501–522. © Glasgow Mathematical Journal Trust 2011.
doi:10.1017/S0017089511000097.

A DIOPHANTINE FROBENIUS PROBLEM RELATED TO RIEMANN SURFACES

CORMAC O'SULLIVAN and ANTHONY WEAVER

Department of Mathematics and Computer Science, Bronx Community College, City University of New York, 2155 University Avenue, Bronx, New York 10453, USA
e-mails: cormac.osullivan@bcc.cuny.edu; anthony.weaver@bcc.cuny.edu

(Received 9 March 2010; accepted 30 November 2010; first published online 10 March 2011)

Abstract. We obtain sharp upper and lower bounds on a certain four-dimensional Frobenius number determined by a prime pair (p, q), $2 < p < q$, including exact formulae for two infinite subclasses of such pairs. Our work is motivated by the study of compact Riemann surfaces which can be realised as semi-regular pq-fold coverings of surfaces of lower genus. In this context, the Frobenius number is (up to an additive translation) the largest genus in which no surface is such a covering. In many cases it is also the largest genus in which no surface admits an automorphism of order pq. The general t-dimensional Frobenius problem ($t \geq 3$) is NP-hard, and it may be that our restricted problem retains this property.

2010 *Mathematics Subject Classification.* Primary 14J50, 11D04.

1. Introduction. A set of integers $\{a_1, a_2, \dots a_t\}$, $t \geq 2$, with $a_i > 1$ and gcd $= 1$, has a *Frobenius number*

$$g(\{a_1, a_2, \dots, a_t\}),$$

which is the largest positive integer not representable in the form $k_1a_1 + k_2a_2 + \cdots + k_ta_t$, where each k_i is a non-negative integer. It is a simple exercise to show that $g(\{a_1, a_2, \dots, a_t\})$ exists under the stated conditions. Finding $g(\{a_1, \dots, a_t\})$ for a given set $\{a_1, \dots, a_t\}$ is the linear Diophantine Frobenius problem [**11**]. In 1884, Sylvester [**12**] established the formula

$$g(\{a_1, a_2\}) = a_1a_2 - a_1 - a_2 \tag{1.1}$$

for the *two-dimensional* Frobenius number. In 1990, it was shown by Curtis [**2**] that for $t \geq 3$ there is no finite set of polynomials $\{f_1, \dots, f_k\}$ in t variables such that, for each t-tuple $\{a_1, a_2, \dots, a_t\}$ with greatest common divisor 1, $g(\{a_1, a_2, \dots, a_t\}) = f_i(a_1, a_2, \dots, a_t)$ for some i. Algorithms for computing the t-dimensional Frobenius numbers exist [**11**], but the problem (for variable $t \geq 3$) is NP-hard [**10**].

Throughout the paper, p, q will be primes satisfying $2 < p < q$ with p', q' denoting the integers $(p-1)/2$ and $(q-1)/2$, respectively. The four integers

$$d_0 = pq, \quad d_1 = p'q, \quad d_2 = pq', \quad d_3 = (pq-1)/2 \tag{1.2}$$

have gcd $= 1$, so they determine the four-dimensional Frobenius number

$$g_{pq} = g(\{d_0, d_1, d_2, d_3\}). \tag{1.3}$$

The significance of the number g_{pq} in (1.3) is that

$$g_{pq} - pq + 1$$

is the largest integer such that no compact Riemann surface of that genus is a semi-regular pq-fold cover of some other surface. This is explained in Section 3. A closely related quantity of interest to us is ν_{pq}, the largest integer such that no compact Riemann surface of that genus has an automorphism group that is cyclic of order pq. ν_{pq} is called the *largest non-genus* of the group $\mathbb{Z}_{pq}$. As a special case of Theorem 3.3 we have

$$g_{pq} - pq + 1 \leq \nu_{pq} \leq g_{pq}. \tag{1.4}$$

Our main results, listed in the next section, yield bounds for g_{pq}. When q is sufficiently large with respect to p, we obtain exact formulas for g_{pq} as well as ν_{pq}. At the other extreme we also give exact formulas for g_{pq} and ν_{pq} when $q = p + 2$.

More generally, as we describe in Section 3, there is a Frobenius number g_n so that $g_n - n + 1$ is the largest possible genus for a compact Riemann surface that is not a semi-regular n-fold cover of another surface. For square-free odd n with $s > 2$ prime factors, this will correspond to a more difficult 2^s-dimensional Frobenius problem. ν_n, the largest non-genus for the cyclic group $\mathbb{Z}_n$, has been found in the case of $n = p^e$ for p prime by Kulkarni and Maclachlan [**7**]. Kulkarni [**6**] showed that, for an arbitrary finite group G, the genera where it is possible for a surface to admit G as an automorphism group form an arithmetic progression. He showed that there also exists largest non-genus in this progression. These genera are studied with generating functions in [**8**].

2. The main results. Define the function

$$\mathfrak{f}_{p,q}(x, y, z, w) = xd_0 + yd_1 + zd_2 + wd_3, \tag{2.1}$$

where the integers d_i are defined in (1.2). A positive integer n is *representable* if $n = \mathfrak{f}_{p,q}(x, y, z, w)$ for x, y, z, w non-negative. The Frobenius number (1.3) is the largest non-representable integer. Since p and q are fixed in all our arguments, we henceforth put $\mathfrak{f} = \mathfrak{f}_{p,q}$, and write g for g_{pq}, suppressing the subscripts.

We define integers $\kappa, \kappa', \lambda, \lambda'$ as follows:

$$q = \kappa p + \lambda, \qquad 1 \leq \lambda \leq p - 1, \tag{2.2}$$

$$q' = \kappa' p' + \lambda', \qquad 0 \leq \lambda' \leq p' - 1. \tag{2.3}$$

The integers

$$G_0 \equiv \mathfrak{f}(p' - 1, p - 1, \kappa, -1), \qquad G_1 \equiv G_0 - \lambda d_3, \qquad G_2 \equiv G_0 - (p - 3)d_3 \tag{2.4}$$

play an important role.

THEOREM 2.1. *The Frobenius number g satisfies*

(i) $G_2 \leq g \leq G_0$,

(ii) $g = G_0$ *if and only if* $\kappa + \lambda \geq p$,

(iii) $g = G_2$ *if* $p = 3$ *or* (p, q) *is a twin prime pair.*

We note that if $p = 3$, then $G_2 = G_0$ and $\kappa + \lambda \geq 3$, so that parts (i) and (ii) of Theorem 2.1 imply that $g = G_0$ (and hence also $g = G_2$, as in part (iii)). For $p > 3$, the

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

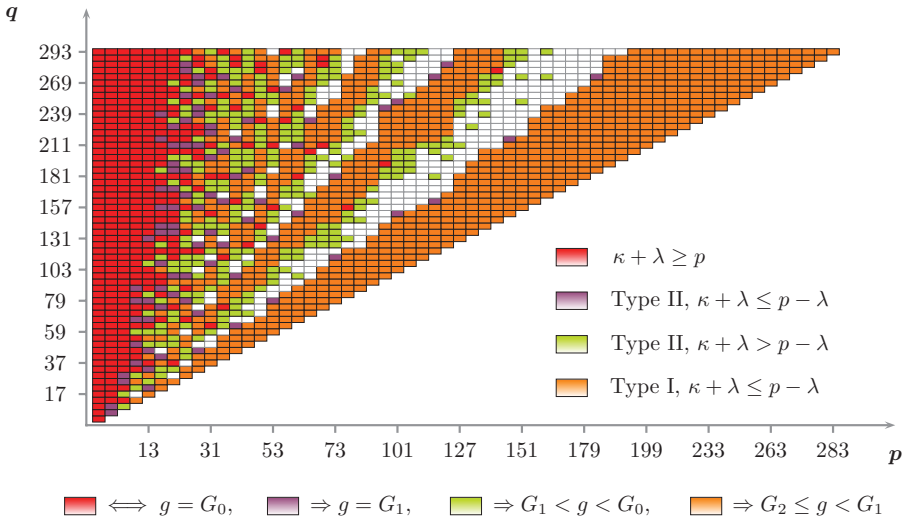

Figure 1. (Colour online) $2 < p < q < 300$.

integer $q = (p-3)p+1$, if prime, is the largest such that $\kappa + \lambda < p$. Hence, we obtain an easy corollary.

COROLLARY 2.2. *If* $q \geq (p-3)p+3$, $g = G_0$.

When $\kappa + \lambda < p$, by Theorem 2.1, $G_2 \leq g < G_0$. These bounds can be tightened in some cases. To treat these cases, we introduce some more notation.

Note that κ and λ have opposite parity (otherwise q is not prime), and $\kappa' \geq \kappa$. If $\kappa + \lambda < p$, then, in fact, $\kappa + \lambda \leq p-2$ and hence $\lambda \leq p-3$. It follows that there is a unique non-negative integer $\tau < \lambda$ such that

$$\frac{\tau+2}{\tau+1} < \frac{p}{\lambda} < \frac{\tau+1}{\tau}. \tag{2.5}$$

We allow $\tau = 0$ so as to include the cases in which $2 < \frac{p}{\lambda}$. (It is also easy to see that $\tau = \lfloor \lambda/(p-\lambda) \rfloor$.) Every pair (p, q) with $\kappa + \lambda < p$ belongs to one of the following two types:

$$\text{Type I.} \quad \frac{\tau+2}{\tau+1} < \frac{p'}{\lambda'}, \qquad \text{Type II.} \quad \frac{p'}{\lambda'} \leq \frac{\tau+2}{\tau+1}. \tag{2.6}$$

THEOREM 2.3. *For a Type II pair, the Frobenius number g satisfies*
(i) $G_1 \leq g < G_0$,
(ii) $g = G_1$ *if and only if* $\kappa + \lambda \leq p - \lambda$.

THEOREM 2.4. *For a Type I pair with* $\kappa + \lambda \leq p - \lambda$, *the Frobenius number g satisfies*
(i) $G_2 \leq g < G_1$,
(ii) $g = G_2$ *if* (p, q) *is a twin prime pair.*

The above theorems indicate where g lies in relation to G_0, G_1 and G_2. Figure 1 shows how these results are distributed over small prime pairs.

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

With (1.4), we may translate the bounds on g into bounds on ν_{pq}. We can do better in the case when $\kappa + \lambda \geq p$, where, by Theorem 2.1, we have $g = G_0$.

THEOREM 2.5. *For primes $3 < p < q$, with $\kappa + \lambda \geq p$ and $q \neq 2p - 1,\ 3p - 2$, we have*

$$\nu_{pq} = G_0 - pq + 1.$$

Thus, ν_{pq} attains the lower bound of (1.4) in this case. For a twin prime pair, ν_{pq} lies about halfway between the bounds of (1.4) (see Theorem 9.2). It appears that the upper bound is not attained for any prime pair.

The Type I pairs that are not covered by Theorem 2.4 (white in Figure 1) are those for which $p > \kappa + \lambda > p - \lambda$ (see Remark 1, Section 7). We plan to treat these pairs in a future paper. For now, we note that the formula for the Frobenius number g_{pq} depends on the number-theoretic relationship between q/p and q'/p'. Making this dependence precise involves the continued fraction

$$\frac{q}{p} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}. \tag{2.7}$$

The condition $\kappa + \lambda \geq p$, appearing in Theorem 2.1(ii), is equivalent to $q_1 + 1 \leq q'/p'$. It appears that the next case is

$$q_1 + \frac{1}{q_2} \leq \frac{q'}{p'} < q_1 + 1,$$

and that an exact, though more complicated, formula for g is also possible in this case. It seems likely that g_{pq} depends on where q'/p' lies in relation to the convergents of (2.7).

3. The motivating problems. If the compact Riemann surface X admits a finite group G of conformal *automorphisms*, then the quotient space $Y = X/G$ is itself a compact Riemann surface, and the quotient map $\Phi : X \to Y$ is a holomorphic *branched covering map* of degree $n = |G|$ (the order of G). This means that Φ is generically n-to-1 (or n-fold), but there is a finite subset $B \subset Y$, called the branch set, over which the fibres have cardinality strictly less than n. The *Riemann–Hurwitz relation*, a linear Diophantine equation, relates the topological data associated with Φ, namely, the genera of the surfaces, the degree of the covering, and the cardinalities of the fibres over the branch set. It is a generalisation of the multiplicative relation between the Euler characteristics of the surfaces, $\chi(X) = n \cdot \chi(Y)$ which holds for n-fold *unbranched* covering maps. (See [**3**], Sections I.1 and I.2, for a fuller treatment of these ideas.)

Branched covering maps need not arise as quotient maps of group actions. Those that do must satisfy an extra regularity condition: for every $y \in B$, there exists a divisor $n_y > 1$ of n such that the fibre over y consists of precisely n/n_y points, at which the n sheets of the covering come together in sets of n_y. The integers n_y, $y \in B$, are called the *branching indices*, and the covering is called *semi-regular*. When $\Phi : X \to Y$ is a

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

semi-regular branched covering, the Riemann–Hurwitz relation is

$$2(\gamma - 1) = 2n(\eta - 1) + n \sum_{y \in B} \left(1 - \frac{1}{n_y}\right), \tag{3.1}$$

where γ, η, are the genera of X, Y, respectively, n is the degree of the covering, and n_y, $y \in B$ are the branching indices. If Φ can be realised as the quotient map of a group action, the covering is called *regular*.

We now specialise to the case where n, the degree of the covering, is a square-free odd integer with $s \geq 1$ distinct prime factors p_i, $i = 1, 2, \ldots, s$. The 2^s divisors of n are in one-to-one correspondence with the set $\mathcal{B}$ of binary bit strings of length s. Let I denote a bit string of length s, and $\overline{0}$, $\overline{1}$ the bit strings consisting of all 0s and all 1s, respectively. Let n_I denote the divisor of n associated with the bit string I, so that, for example, $n_{\overline{0}} = 1$ and $n_{\overline{1}} = n$, and, more generally, p_i is a factor of n_I if and only if the ith bit of I is 1. Then (3.1) implies that the Riemann–Hurwitz formula for an n-fold semi-regular branched covering is

$$\gamma + n - 1 = x_{\overline{0}} n + \sum_{I \neq \overline{0}} x_I \frac{n(n_I - 1)}{2n_I}, \tag{3.2}$$

where x_I $(I \neq \overline{0})$ is the number of points in the branch set with branching index n_I, and $x_{\overline{0}} = \eta$, the genus of Y. The integers

$$d_{\overline{0}} = n, \qquad d_I = \frac{n(n_I - 1)}{2n_I}, \quad I \in \mathcal{B}, I \neq \overline{0}$$

have gcd $= 1$, so there is a 2^s-dimensional Frobenius number $g(\{d_I : I \in \mathcal{B}\})$. By the general theory of branched coverings, there is surface X of genus γ which is an n-fold semi-regular covering if and only if there is a 2^s-tuple $(x_I)_{I \in \mathcal{B}}$ of non-negative integers satisfying (3.2). It follows that there is the largest *non-genus* of a semi-regular n-fold covering, namely, the additive translate $-n + 1 + g(\{d_I : I \in \mathcal{B}\})$ of the 2^s-dimensional Frobenius number $g(\{d_I : I \in \mathcal{B}\})$.

PROBLEM I. For every square-free odd n with s distinct prime factors, determine the largest non-genus of a semi-regular n-fold covering. This genus is $g_n - n + 1$, where g_n is the 2^s-dimensional Frobenius number $g(\{d_I : I \in \mathcal{B}\})$.

The case $s = 1$ of Problem I follows immediately from the previous paragraph and Sylvester's formula (1.1) for the two-dimensional Frobenius number.

PROPOSITION 3.1. *Let p be an odd prime. The largest non-genus of a p-fold semi-regular branched covering is $p'(p-3) - p$, the additive translate $g(\{p, p'\}) - p + 1$ of the two-dimensional Frobenius number $g(\{p, p'\})$.*

Note that this integer is < 0 for $p = 3, 5$, so that there is a semi-regular three- or five-fold branched covering of every genus.

3.1. Group actions. We now give a set of necessary and sufficient conditions for the existence of a *regular cyclic* n-fold branched covering $\Phi : X \to Y$, that is, a covering realisable as the quotient map of a cyclic group $\mathbb{Z}_n$ of automorphisms acting on the compact Riemann surface X. The conditions are a special case of a

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

more general set of conditions for the existence of an action by an arbitrary finite group G of order n. The necessary and sufficient condition in the general case is the existence of a *partial monodromy presentation* of G, having a form dictated by the genus of Y and the branching indices. If the genus of Y is η, and the branching indices are $r_1, r_2, \ldots, r_k$, the monodromy presentation of G must have $2\eta + k$ generators $a_1, b_1, \ldots, a_\eta, b_\eta, c_1, \ldots, c_k$, where c_i has order r_i and, among other possible relations,

$$\prod_{i=1}^{\eta}[a_i, b_i]\prod_{j=1}^{k} c_j = 1, \tag{3.3}$$

where $[a_i, b_i]$ denotes the commutator and 1 denotes the identity element in G. (For a fuller explanation of the general case, see, for example, [**1**] or [**9**, Chapter III, Section 3] or [**4**, Section 1.7].)

LEMMA 3.2. *Let $n = p_1, \ldots, p_s$, $s \geq 1$, a square-free odd integer with prime factors $p_1, \ldots, p_s$. Let $\gamma \geq 0$. Let $(x_I \geq 0)_{I\in\mathcal{B}}$ be a 2^s-tuple satisfying* (3.2) *for n, γ. There is a compact Riemann surface of genus γ admitting a group of automorphisms $\mathbb{Z}_n$ such that quotient surface has genus $x_{\overline{0}}$ and x_I points of branching indices n_I, $I \neq \overline{0}$, if and only if the tuple $(x_I \geq 0)_{I\in\mathcal{B}}$ satisfies the admissibility conditions*

$$\sum_{I\in\mathcal{B}^i} x_I \neq 1, \quad i = 1, 2, \ldots, s, \tag{3.4}$$

$$x_{\overline{0}} + \sum_{I\in\mathcal{B}^i} x_I \neq 0, \quad i = 1, 2, \ldots, s, \tag{3.5}$$

where $\mathcal{B}^i \subset \mathcal{B}$ is the set of bit strings of length s whose ith bit is 1.

Proof. A partial monodromy presentation of $\mathbb{Z}_n$ dictated by the tuple $(x_I \geq 0)_{I\in\mathcal{B}}$ would have $2x_{\overline{0}}$ generators $a_0, b_0, \ldots, a_{x_{\overline{0}}}, b_{x_{\overline{0}}}$ of unspecified order, and x_I generators c_I of order n_I for each $I \in \mathcal{B}$, $I \neq \overline{0}$. Since all commutators are trivial in an abelian group, the elements a_j, b_j can be omitted from the relation (3.3). If the ith condition in (3.4) fails, then the group product on the left-hand side of (3.3) would contain exactly one element of order divisible by p_i, and hence could not be equal to the identity. If the ith condition in (3.5) fails, the generating set would contain no elements of order divisible by p_i, a contradiction. This proves the necessity of the conditions. To prove sufficiency of the conditions, one verifies that a partial monodromy presentation of $\mathbb{Z}_n$ can be constructed in all other cases; this is left as an exercise. □

If there exist tuples $(x_I \geq 0)_{I\in\mathcal{B}}$ satisfying (3.2) for some γ, n, but none of them satisfy all the admissibility conditions in (3.4) and (3.5), then γ is the genus of an n-fold semi-regular covering, but a *non-genus* for a $\mathbb{Z}_n$ action. There exists a largest non-genus of a $\mathbb{Z}_n$ action [**6**], and it must be at least as large as the largest non-genus of an n-fold semi-regular covering.

PROBLEM II. For every square-free odd n, determine the largest non-genus ν_n of $\mathbb{Z}_n$.

THEOREM 3.3. *Let n be a square-free odd integer with $s \geq 1$ distinct prime factors. With ν_n denoting the largest non-genus of a $\mathbb{Z}_n$ action, and g_n the Frobenius number $g(\{d_I : I \in \mathcal{B}\})$, we have*

$$g_n - n + 1 \leq \nu_n \leq g_n. \tag{3.6}$$

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

Proof. The left-hand inequality is clear: $\gamma = g_n - n + 1$ is the largest integer such no 2^s-tuple $(x_I)_{I\in\mathcal{B}}$ (admissible or not) satisfies (3.2). Hence, ν_n must be at least as large as $g_n - n + 1$. For the right-hand inequality, let $(x_I)_{I\in\mathcal{B}}$ be a non-negative 2^s-tuple satisfying (3.2) for some γ. The tuple obtained from (x_I) by replacing the final coordinate $x_{\bar{1}}$ with $x_{\bar{1}} + 2$ satisfies (3.2) with γ replaced by $\gamma + n - 1$. Moreover, the new tuple satisfies the admissibility conditions (3.4) and (3.5). Thus, if there is a surface of genus γ, which is an n-fold semi-regular covering, there is a surface of genus $\gamma + n - 1$ that admits a $\mathbb{Z}_n$ action. Consequently, ν_n is no larger than $g_n - n + 1 + n - 1 = g_n$. □

In the case $s = 1$, the Riemann–Hurwtiz relation is

$$\gamma + p - 1 = x_0 p + x_1 p', \tag{3.7}$$

and the admissibility conditions are simply $x_0 + x_1 \neq 0$ and $x_1 \neq 1$. It is easy to verify that there is just one solution for (3.7) when $\gamma = g(\{p, p'\})$, namely, the inadmissible pair $(x_0, x_1) = (p' - 1, 1)$. Thus, the largest non-genus of a $\mathbb{Z}_p$ action is strictly greater than the largest non-genus of a semi-regular p-fold covering (cf. Proposition 3.1). In fact it is known ([**7**]) that $\nu_p = g(\{p, p'\}) = g_p$. This shows that the upper bound in (3.6) can be attained. We conjecture that $s = 1$ is the only case in which this occurs. We shall show in Section 9 that when $s = 2$, the lower bound in (3.6) is attained for infinitely many $n = pq$.

A group of square-free order is either cyclic or metacyclic (see, for example, [**5**], Theorem 9.4.3). A metacyclic group has a normal cyclic subgroup with a cyclic factor group. If $s = 1$, the only possible group is $\mathbb{Z}_p$. If $s = 2$, there is a (non-abelian) metacyclic group (of order pq) if and only if p is a divisor of $q - 1$. Such a group contains no elements of order pq; hence, the quotient map has no branching indices equal to pq, and the corresponding Frobenius problem is three-dimensional, not four-dimensional. The admissibility conditions for a partial monodromy presentation are (naturally) different. A formula for the largest non-genus of a metacyclic group action of order pq is given by the second author in [**13**]. In Section 9 we give a formula for the largest non-genus of $\mathbb{Z}_{pq}$, which, given p, is valid for all but finitely many $q > p$.

Henceforth we treat Problems I and II exclusively for n a product of two distinct primes. Until the last section, we revert to the purely number-theoretic question of determining the four-dimensional Frobenius number $g = g(\{d_0, d_1, d_2, d_3\})$, with d_i as defined in (1.2).

4. Representability of integers $> G_0$. To prove that a certain integer m is the Frobenius number g, we need to establish that (a) m is not representable as $\mathfrak{f}(x, y, z, w)$ for any quadruple (x, y, z, w) of non-negative integers; and (b) all integers $> m$ are representable in this way. For (b), it suffices to show that all integers in the closed interval $[m + 1,\ m + d_1]$ are representable, since if $\mathfrak{f}(x, y, z, w)$ is a non-negative representation of $k \in [m + 1, m + d_1]$, then $\mathfrak{f}(x, y + l, z, w)$ is a non-negative representation of $k + ld_1$, for any $l \geq 0$. In this and subsequent sections we apply this method to $m = G_0,\ G_1$ and G_2, as they are defined in (2.4). Having applied the method to G_0, it will be possible to reuse much of the work in the treatment of G_1 and G_2.

For $x, y, z, w \in \mathbb{Q}$, the equation $\mathfrak{f}(x, y, z, w) = 0$ determines the three-dimensional vector subspace of $\mathbb{Q}^4$, whose span is the hyperplane orthogonal to the vector

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

(d_0, d_1, d_2, d_3). It has an obvious basis consisting of the following three vectors:

$$(d_1, -d_0, 0, 0), \quad (0, d_2, -d_1, 0), \quad (0, 0, d_3, -d_2).$$

It is easy to show that

$$e_0 = (p', -p, 0, 0), \tag{4.1}$$
$$e_1 = (p', 0, 1, -p), \tag{4.2}$$
$$e_2 = (q', 1, 0, -q), \tag{4.3}$$

are also a basis. This basis is convenient since (an exercise shows) if there are integer quadruples (x, y, z, w) and (x', y', z', w') such that $\mathfrak{f}(x, y, z, w) = \mathfrak{f}(x', y', z', w')$, then the vector $(x - x', y - y', z - z', w - w')$ is an *integer* linear combination of e_0, e_1 and e_2. Thus, since $\mathfrak{f}$ is linear, $\mathfrak{f}(x, y, z, w) = \mathfrak{f}(x', y', z', w')$ if and only if $(x', y', z', w') = (x, y, z, w) + \alpha e_1 + \beta e_2 + \gamma e_3$, for some $\alpha, \beta, \gamma \in \mathbb{Z}$.

PROPOSITION 4.1. *All integers $> G_0$ are representable.*

To prove this, we show that for each integer n in the closed interval $[G_0 + 1, G_0 + d_1]$, a non-negative quadruple (x, y, z, w) exists such that $\mathfrak{f}(x, y, z, w) = n$. We first construct quadruples (possibly with negative entries) representing the integers in $[G_0 + 1, G_0 + d_1]$ and then show that they can be altered, if necessary, by adding an integer linear combination of the vectors e_0, e_1, e_2, so that they become *non-negative* quadruples. We will make use of the following easily verified facts:

$$\mathfrak{f}(0, -1, 0, 1) = q', \tag{4.4}$$
$$\mathfrak{f}(0, 0, -1, 1) = p', \tag{4.5}$$
$$\mathfrak{f}(1, 0, 0, -2) = 1. \tag{4.6}$$

We start by obtaining a non-negative representation of $G_0 + 1$, using $\mathfrak{f}(e_1) = 0$ and (4.6):

$$\begin{aligned} G_0 + 1 &= \mathfrak{f}(p' - 1, p - 1, \kappa, -1) - \mathfrak{f}(p', 0, 1, -p) + \mathfrak{f}(1, 0, 0, -2) \\ &= \mathfrak{f}(0, p - 1, \kappa - 1, p - 3). \end{aligned} \tag{4.7}$$

We proceed to show that $G_0 + 1 + t$ has a non-negative representation for all $t \in [0, d_1 - 1]$.

Let an integer $t \in [0, d_1 - 1]$ be represented with the division algorithm as

$$t = aq' + bp' + c, \quad \text{with} \quad a \geq 0 \text{ maximal}, \quad b \geq 0, \quad 0 \leq c \leq p' - 1. \tag{4.8}$$

The triple (a, b, c) is uniquely determined by t and conversely.

LEMMA 4.2. *If $t \in [0, d_1 - 1]$ has the representation* (4.8)*, then*

(i) $a \leq p - 1$;
(ii) $a = p - 1 \implies b = 0$;
(iii) $b \leq \kappa'$,
(iv) $b = \kappa' \implies c < \lambda' \implies p > 3$,
(v) $b \geq \kappa \implies a \leq p - 2$.

Proof. (i) and (v): If $a \geq p$, or if $a = p - 1$ and $b \geq \kappa$, then $t \geq p'q = d_1$, contrary to assumption. (ii): If $a = p - 1$ and $t \leq p'q$, then $bp' + c \leq p' - 1$, which implies $b = 0$.

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

(iii): If $b > \kappa'$, a is not maximal. (iv): If $b = \kappa'$ and $c \geq \lambda'$, a is not maximal. When $p = 3$, $\lambda' = 0$ and hence $c < \lambda'$ is impossible. □

It follows from (4.4)–(4.6) that for $t \in [0, d_1 - 1]$,

$$G_0 + 1 + t = \mathfrak{f}(0, p-1, \kappa-1, p-3) + a \cdot \mathfrak{f}(0, -1, 0, 1) + b \cdot \mathfrak{f}(0, 0, -1, 1) + c \cdot \mathfrak{f}(1, 0, 0, -2).$$

Thus $G_0 + 1 + t = \mathfrak{f}(x,\ y,\ z,\ w)$, where

$$x = c, \tag{4.9}$$
$$y = p - 1 - a, \tag{4.10}$$
$$z = \kappa - 1 - b, \tag{4.11}$$
$$w = p - 3 - 2c + a + b. \tag{4.12}$$

By definition, $x \geq 0$. By Lemma 4.2(i), $y \geq 0$, and $w \geq 0$ because $c \leq p' - 1$ is equivalent to

$$p - 3 - 2c \geq 0. \tag{4.13}$$

Thus, z is the only component of the quadruple (x, y, z, w), which might be negative (if $b \geq \kappa$). If this is the case, then

$$b = \kappa + s \quad \text{for some} \quad 0 \leq s \leq \kappa' - \kappa. \tag{4.14}$$

The upper bound on s is a consequence of Lemma 4.2(iii). We now show that there is always an integer linear combination of the vectors (4.2) and (4.3), which when added to the quadruple defined by (4.9)–(4.12) yields a non-negative quadruple. The argument will be divided into three parts (Lemmas 4.3, 4.4 and 4.5) according to whether s is, respectively, less than, equal to, or greater than $\kappa' - \kappa - 1$.

For notational convenience, we define the quadruple

$$e(u, v) \equiv (u-1)e_2 + (v+1)e_1, \tag{4.15}$$

where e_1 and e_2 are the vectors (4.2) and (4.3), respectively, and $u, v \in \mathbb{Z}$.

LEMMA 4.3. *If* $s < \kappa' - \kappa - 1$,
(i) $\kappa + s - (s+1)p \geq 0$;
(ii) $(x', y', z', w') = (x, y, z, w) + e(1, s)$ *is a non-negative quadruple.*

Proof. From $q' \geq \kappa' p'$ we obtain $q - 1 \geq \kappa'(p-1) \iff \kappa' - 1 \geq \kappa' p - q = (\kappa' - \kappa)p + \kappa p - q$, and hence

$$\kappa' - 1 \geq (\kappa' - \kappa)p - \lambda.$$

It follows from this that

$$\kappa' - 1 - l \geq (\kappa' - \kappa)p - \lambda - l, \quad \text{for} \quad l \geq 0.$$

In particular, since $\lambda \leq p - 1$,

$$\kappa' - 1 - l \geq (\kappa' - \kappa)p - lp \quad \text{if} \quad l \geq 1. \tag{4.16}$$

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

Putting $l = \kappa' - \kappa - s - 1 \geq 1$ in (4.16), we obtain (i). To prove (ii), we have $x' > x \geq 0$, $y' = y \geq 0$, and $z' = -(s+1) + (s+1) = 0$. We need only show that

$$w' = p - 3 - 2c + a + b - (s+1)p \tag{4.17}$$

is non-negative. Recalling that $b = \kappa + s$, and using (4.13), we obtain

$$w' \geq \kappa + s - (s+1)p.$$

Thus, $w' \geq 0$ is a consequence of (i). □

If $s = \kappa' - \kappa - 1$, then $w \geq (s+1)p$ easily implies that the fourth coordinate of $(x, y, z, w) + e(1, s)$ is positive. The following lemma treats the case $w < (s+1)p$, where the fourth coordinate of $(x, y, z, w) + e(1, s)$ is negative.

LEMMA 4.4. *If* $s = \kappa' - \kappa - 1$ and $w < (s+1)p$, then

(i) $c - \lambda' \geq 0$;
(ii) $(x', y', z', w') = (x, y, z, w) + e(0, \kappa' - 1)$ *is a non-negative quadruple.*

Proof. $w = p - 3 - 2c + a + \kappa + s < (s+1)p$ is equivalent to

$$\begin{aligned} 2c &> \kappa - 3 - s(p-1), \\ c &> (\kappa - 3)/2 - sp', \\ c &\geq (\kappa - 1)/2 - sp'. \end{aligned}$$

Putting $s = \kappa' - \kappa - 1$, we have

$$\begin{aligned} c &\geq (\kappa - 1 + p - 1)/2 - (\kappa' - \kappa)p' \\ &\geq (\kappa + \lambda - 1)/2 - (\kappa' - \kappa)p' \\ &= \lambda', \end{aligned}$$

where we have used $\lambda \leq p - 1$ and Lemma 7.1. Thus, (i) is proved. $x' = c - \lambda'$, which is ≥ 0 by (i). $y' = p - 1 - a - 1 \geq 0$ by Lemma 4.2(v). $z' = -s - 1 + \kappa' = \kappa \geq 1$. Finally, $w' = w + q - k'p = w - (\kappa' - \kappa)p + \lambda$. Since $w \geq b = \kappa + s = \kappa' - 1$, and $\kappa' - 1 \geq (\kappa' - \kappa)p - \lambda$ by (4),

$$w' = w - (\kappa' - \kappa)p + \lambda \geq (\kappa' - \kappa)p - \lambda - (\kappa' - \kappa)p + \lambda = 0.$$

Thus, (ii) is proved. □

LEMMA 4.5. *If* $s = \kappa' - \kappa$, *then* $(x', y', z', w') = (x, y, z, w) + e(0, \kappa')$ *is a non-negative quadruple.*

Proof. By Lemma 4.2(iv), $c < \lambda'$. Since both c and λ' are $\leq p' - 1$,

$$1 \leq \lambda' - c \leq p' - 1. \tag{4.18}$$

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

We have

$$x' = c - q' + (\kappa' + 1)p' = p' - (\lambda' - c), \tag{4.19}$$
$$y' = p - 2 - a, \tag{4.20}$$
$$z' = -(s + 1) + \kappa' + 1 = \kappa, \tag{4.21}$$
$$\begin{aligned} w' &= p - 3 - 2c + a + \kappa' + q - (\kappa' + 1)p \\ &= -3 - 2c + a + q - \kappa'(p - 1) \\ &= -2 - 2c + a + q - 1 - \kappa'(p - 1) \\ &= -2 - 2c + a + 2(q' - \kappa' p') \\ &= -2 - 2c + a + 2\lambda' \\ &= 2(\lambda' - c) - 2 + a, \end{aligned} \tag{4.22}$$

$x', w' \geq 0$ by (4.18). $y' \geq 0$ by Lemma 4.2(v). Finally, $z' = \kappa \geq 1$. □

Lemmas 4.3, 4.4 and 4.5 together constitute a proof of Proposition 4.1, which implies that $g \leq G_0$ for all prime pairs $2 < p < q$.

5. Representability of G_0. In this section we prove the following.

PROPOSITION 5.1. *G_0 is representable if and only if $\kappa + \lambda < p$.*

Suppose $\kappa + \lambda < p$, and put $(x', y', z', w') = e(0, \kappa' - 1) + (p' - 1, p - 1, \kappa, -1)$. Since

$$e(0, \kappa' - 1) = (-q' + \kappa' p', -1, \kappa', q - \kappa' p) = (-\lambda', -1, \kappa, \lambda) \tag{5.1}$$

(the last equality being a consequence of $\kappa' = \kappa$), it easily verified that (x', y', z', w') is a non-negative quadruple representing G_0.

To prove the necessity of the condition, we employ a number-theoretic lemma whose proof is a simple exercise.

LEMMA 5.2. *Let m, n be relatively prime integers. If $am + bn = a'm + b'n$ for any $a, a', b, b' \in \mathbb{Z}$, then there exists an integer l such that $a' = a - ln$ and $b' = b + lm$.*

PROPOSITION 5.3. *If (x_0, y_0, z_0, w_0) and (x, y, z, w) are integer quadruples such that $\mathfrak{f}(x_0, y_0, z_0, w_0) = \mathfrak{f}(x, y, z, w)$, there exists an integer l such that the system*

$$\begin{cases} x_0 p + (y_0 + w_0)p' - lq' = xp + (y + w)p' \\ z_0 p + w_0 + lq = zp + w \end{cases}$$

is satisfied.

Proof. Using (2.1) and (1.2), we have

$$\begin{aligned} \mathfrak{f}(x_0, y_0, z_0, w_0) &= x_0 pq + y_0 p' q + z_0 pq' + w_0(p'q + q') \\ &= q[x_0 p + (y_0 + w_0)p'] + q'[z_0 p + w_0]. \end{aligned} \tag{5.2}$$

Since q and q' are relatively prime, we can apply Lemma 5.2 with a, b being the two expressions in square brackets in (5.2). □

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

We now resume the proof of Proposition 5.1. Suppose $G_0 = \mathfrak{f}(x, y, z, w)$ with x, y, z, w being non-negative, and further suppose (for a contradiction) that $\kappa + \lambda \geq p$ (equivalently, $\kappa' - \kappa > 0$). Using Proposition 5.3 with $(x_0, y_0, z_0, w_0) = (p' - 1, p - 1, \kappa, -1)$, there exists an integer l such that

$$\begin{cases} (p'-1)p + (p-2)p' - lq' = xp + (y+w)p' \\ \kappa p - 1 + lq = zp + w. \end{cases} \tag{5.3}$$

The second equation implies $l \geq 0$, since the right-hand side is non-negative (by assumption) and $\kappa p - 1 < q$. To simplify the system (5.3), we express q' in terms of p' and p. We have

$$\begin{aligned} q' &= \kappa' p' + \lambda' \\ &= (\kappa' - 2\lambda')p' + 2\lambda' p' + \lambda' \\ &= (\kappa' - 2\lambda')p' + \lambda' p, \end{aligned}$$

where, at the last step, we use $p = 2p' + 1$. By Lemma 7.1, $2\lambda' = \kappa + \lambda - 1 - (\kappa' - \kappa)(p-1)$, and hence

$$q' = Bp' + \lambda' p, \tag{5.4}$$

where

$$B = (\kappa' - \kappa)p - \lambda + 1. \tag{5.5}$$

Since $\kappa' - \kappa > 0$ and $\lambda < p$, B is positive.

Using (5.4), the first equation of (5.3) becomes

$$(p' - 1 - l\lambda')p + (p - 2 - lB)p' = xp + (y+w)p'. \tag{5.6}$$

Since p and p' are relatively prime, Lemma 5.2 applies to the left-hand side, with a and b being the two expressions in parentheses. Hence there exists $t \in \mathbb{Z}$ such that

$$\begin{aligned} x &= p' - 1 - l\lambda' + tp', \\ y + w &= p - 2 - lB - tp. \end{aligned} \tag{5.7}$$

The first equation implies that $t \geq 0$ (otherwise $x < 0$) and the second that $t \leq 0$ (otherwise $y + w < 0$). Hence, $t = 0$. Putting $q = \kappa p + \lambda$ into the second equation of the system (5.3), we see that $w \equiv l\lambda - 1 \pmod{p}$. By (5.7), $y + w \leq p - 2$ and, in particular, since y and w are non-negative, $w \leq p - 2$. The only possibility is $w = l\lambda - 1$. Hence,

$$\begin{aligned} y &= p - 2 - lB - l\lambda + 1 \\ &= p - 1 - l[(\kappa' - \kappa)p + 1] \\ &\geq p - 1 - l(p+1) \end{aligned} \tag{5.8}$$

(since $\kappa' - \kappa > 0$). $y \geq 0$ requires $l = 0$, and $w \geq 0$ requires $l > 0$, a contradiction.

This completes the proof of Proposition 5.1. Combining this with Proposition 4.1, we obtain Theorem 2.1(ii).

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

6. Representability of integers $> G_1$. In this section and the next we recycle, as far as possible, the arguments in Sections 4 and 5, replacing G_0 by G_1. Since $G_1 = G_0 - \lambda d_3$, we attempt this by simply reducing the fourth coordinate of each quadruple by λ. The obstruction, of course, is that some of the fourth coordinates thereby become negative.

PROPOSITION 6.1. *If $\kappa + \lambda \leq p - \lambda$, all integers $> G_1$ are representable.*

Proof. It suffices to show that there is a non-negative quadruple representing each integer in the closed interval $[G_1 + 1, G_1 + d_1]$. We start with the representation $G_1 + 1 = \mathfrak{f}(0, p-1, \kappa - 1, p - 3 - \lambda)$, obtained from (4.7) by subtracting λ from the fourth coordinate. The fact that $\kappa + \lambda$ is odd and less than p, and that $\kappa \geq 1$, together imply that $\lambda \leq p - 3$; thus this is a non-negative representation. Representing $t \in [0, d_1 - 1]$ by (4.8), we write $G_1 + 1 + t = \mathfrak{f}(x, y, z, w)$, where x, y, z are given by (4.9), (4.10), (4.11), respectively, and

$$w = p - 3 - 2c + a + b - \lambda, \tag{6.1}$$

which is obtained from (4.12) by subtracting λ.

If $z \geq 0$, the possible obstruction is $w < 0$. Then $a \leq \lambda$ (since $p - 3 - 2c \geq 0$). Adding (5.1) to (x, y, z, w) yields a non-negative quadruple, provided $c \geq \lambda'$. If $c < \lambda'$,

$$\begin{aligned} w &\geq p - 3 - 2(\lambda' - 1) + a + b - \lambda \\ &= p - 3 - (\kappa + \lambda - 3) + a + b - \lambda \\ &\geq p - \lambda - (\kappa + \lambda) \\ &\geq 0, \end{aligned}$$

contrary to the assumption that $w < 0$.

If $z < 0$, then $b = \kappa$ and $c < \lambda'$. We write $G_1 + 1 + t = \mathfrak{f}(x', y', z', w')$, where x', y', z' are given by (4.19), (4.20), (4.21), respectively, and

$$w' = 2(\lambda' - c) - 2 + a - \lambda, \tag{6.2}$$

which is obtained from (4.22) by subtracting λ. The only possible obstruction is $w' < 0$. If this is the case, we add (5.1) to (x', y', z', w'), yielding the quadruple

$$\begin{aligned} x'' &= p' - 2\lambda' + c, \\ y'' &= p - 3 - a, \\ z'' &= 2\kappa, \\ w'' &= 2(\lambda' - c) - 2 + a. \end{aligned}$$

The assumption $w' < 0$ implies $a < \lambda \leq p - 3$, so that $y'' \geq 0$. Clearly $z'' \geq 0$. $w'' \geq 0$ since it is equal to (4.22). If $x'' < 0$, then $c < 2\lambda' - p'$. If this is the case, then

$$\begin{aligned} w' &\geq 2(\lambda' - (2\lambda' - p' - 1)) - 2 + a - \lambda \\ &\geq 2p' - 2\lambda' - \lambda \\ &= 2p' - (\kappa + \lambda - 1) - \lambda \\ &= p - \lambda - (\kappa + \lambda) \\ &\geq 0, \end{aligned}$$

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

contradicting the assumption that $w' < 0$. Hence, (x'', y'', z'', w'') is a non-negative quadruple. □

COROLLARY 6.2. *If* $\kappa + \lambda \leq p - \lambda$, *then* $g \leq G_1$.

To complete the proofs of Theorems 2.3 and 2.4, we need necessary and sufficient conditions for the representability of G_1, and conditions under which there is an integer $> G_1$, which is not representable.

7. Representability of G_1 and $G_1 + \lambda'$. We need two preliminary results.

LEMMA 7.1. $\lambda' = \dfrac{\kappa + \lambda - 1}{2} - (\kappa' - \kappa)p'$.

Proof. By definition $q - \lambda = \kappa p$, from which we obtain

$$\begin{aligned}(q-1) - \lambda &= \kappa(p-1) + \kappa - 1,\\ q' - \kappa p' &= \frac{\kappa + \lambda - 1}{2},\\ q' - \kappa' p' &= \frac{\kappa + \lambda - 1}{2} - (\kappa' - \kappa)p'.\end{aligned}$$

The left-hand side of the last equation is the definition of λ'. □

LEMMA 7.2. *If* $\kappa + \lambda < p$, *then*

(i) $\kappa = \kappa'$;

(ii) $\lambda' = \dfrac{\kappa + \lambda - 1}{2} \geq 1$;

(iii) $\dfrac{p'}{\lambda'} < \dfrac{p}{\lambda}$.

Proof. Using the formula for λ' given in Lemma 7.1 and the assumption that $\kappa + \lambda < p$, we have $\lambda' < p' - (\kappa' - \kappa)p'$. Since $\kappa' - \kappa \geq 0$ and $\lambda' \geq 0$, the only possibility is (i). The equality in (ii) follows from (i) and Lemma 7.1. The right-hand inequality follows from $\kappa + \lambda \geq 3$. To prove (iii), suppose $\frac{p'}{\lambda'} \geq \frac{p}{\lambda}$. Then $p'\lambda \geq p\lambda'$, and hence using (ii),

$$\begin{aligned}2p'\lambda &\geq p(2\lambda'),\\ (p-1)\lambda &\geq p(\kappa + \lambda - 1),\\ -\lambda &\geq p(\kappa - 1) \geq 0,\end{aligned}$$

a contradiction. □

Suppose $G_1 = \mathfrak{f}(x, y, z, w)$ with x, y, z, w being non-negative. Using Proposition 5.3 with $(x_0, y_0, z_0, w_0) = (p' - 1, p - 1, \kappa, -1 - \lambda)$, there exists an integer l such that

$$\begin{cases}(p'-1)p + (p-2)p' - lq' = xp + (y+w)p',\\ \kappa p - 1 - \lambda + lq = zp + w.\end{cases} \tag{7.1}$$

The second equation implies $l \geq 0$ (and the first that l cannot be too large). Imitating the argument leading from (5.3) to (5.7), we see that there exists an integer $t \geq 0$ such

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

that

$$x = p' - 1 - l\lambda' + tp', \tag{7.2}$$

$$y + w = p - 2 - l + \lambda(l-1) - tp. \tag{7.3}$$

(We used B as defined in (5.5), but with $\kappa' - \kappa = 0$.) From the second equation of (7.1) (putting $q = \kappa p + \lambda$), we see that $w \equiv (l-1)\lambda - 1 \pmod{p}$. Then (7.3) yields $y \equiv p - 1 - l \pmod{p}$. Hence there exist $\mu, \nu \in \mathbb{Z}$ such that

$$\begin{aligned} y &= \nu p + p - 1 - l \\ w &= \mu p + (l-1)\lambda - 1. \end{aligned} \tag{7.4}$$

By (7.3), $\mu + \nu = -t$. $\nu \geq 0$ from the assumption that $y \geq 0$. Provided that $l \leq p - 1$ (we shall see shortly that this assumption is justified), we may add a suitable multiple of (4.1) to (x, y, z, w), and so assume $\nu = 0$. Then $\mu = -t$. From (7.4) and the second equation of (7.1),

$$z = (l+1)\kappa + t.$$

Thus a quadruple representing G_1 has the general form

$$\begin{aligned} x &= p' - 1 - l\lambda' + tp' \qquad (0 \leq t, \quad 0 \leq l \leq p-1), \\ y &= p - (l+1), \\ z &= (l+1)\kappa + t, \\ w &= -tp + (l-1)\lambda - 1. \end{aligned} \tag{7.5}$$

($t = l = 0$ yields the defining representation of G_1.)

PROPOSITION 7.3. *G_1 is representable if and only if the pair is of Type I.*

Proof. If the pair is of Type I, let $t = \tau$ and $l = \tau + 2$ in (7.5). Then $x = (\tau+1)p' - (\tau+2)\lambda' - 1$ is non-negative as a consequence of $\frac{\tau+2}{\tau+1} < \frac{p'}{\lambda'}$, and $w = -\tau p + (\tau+1)\lambda - 1$ is non-negative as a consequence of $\frac{p}{\lambda} < \frac{\tau+1}{\tau}$. Obviously $z \geq 0$. It remains only to verify that $l \leq p - 1$, so that $y \geq 0$. $\kappa + \lambda < p$ implies $\lambda \leq p - 3$, and $\tau < \lambda$, so that $l = \tau + 2 < \lambda + 2 \leq p - 1$.

Suppose the pair is of Type II and t and l are non-negative integers making (7.5) a non-negative quadruple. $x \geq 0$, $w \geq 0$ imply, respectively,

$$\frac{l}{t+1} < \frac{p'}{\lambda'}, \quad \text{and} \quad \frac{p}{\lambda} < \frac{l-1}{t}.$$

It follows that $l > t + 1$, and in particular,

$$\frac{t+2}{t+1} \leq \frac{l}{t+1} < \frac{p'}{\lambda'}, \quad \text{and} \quad \frac{p}{\lambda} < \frac{t+1}{t} < \frac{l-1}{t}. \tag{7.6}$$

Since the pair is of Type II, the left-hand inequality implies $t > \tau$, while the right-hand inequality, by the definition of τ, implies that $t \leq \tau$, a contradiction. □

From Corollary 6.2 and Proposition 7.3, we obtain the following.

COROLLARY 7.4. *If the pair is of Type II with $\kappa + \lambda \leq p - \lambda$, then $g = G_1$. If the pair is of Type I with $\kappa + \lambda \leq p - \lambda$, then $g < G_1$.*

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

The next proposition treats the remaining Type II pairs, and completes the proofs of all statements regarding G_0 and G_1 in Theorems 2.1, 2.3 and 2.4.

PROPOSITION 7.5. *If the pair is of Type II with $\kappa + \lambda > p - \lambda$, then $G_1 + \lambda'$ is not representable and hence $g > G_1$.*

Proof. Suppose $G_1 + \lambda' = \mathfrak{f}(x, y, z, w)$ for a non-negative quadruple (x, y, z, w). A general form for (x, y, z, w) is produced from (7.5) by using (4.6) to write $G_1 + \lambda' = G_1 + \lambda' \cdot \mathfrak{f}(1, 0, 0, -2)$. Reducing the fourth coordinate of (7.5) by $2\lambda' = \kappa + \lambda - 1$ (Lemma 7.2(ii)), and increasing the first by λ', we obtain

$$\begin{aligned} x &= p' - 1 - (l-1)\lambda' + tp' \qquad (0 \le t, \quad 0 \le l \le p-1), \\ y &= p - (l+1), \\ z &= (l+1)\kappa + t, \\ w &= -tp + (l-2)\lambda - \kappa. \end{aligned} \tag{7.7}$$

The assumptions $x \ge 0$ and $w \ge 0$ imply almost the same inequalities as in (7.6), except that l is replaced by $l - 1$ where it occurs. Regardless, we arrive at the same contradiction ($t > \tau$ and $t \le \tau$) which concluded the proof of Proposition 7.3. □

REMARK 1. For the remaining Type I pairs (having $\kappa + \lambda > p - \lambda$ and coloured white in Figure 1), both $g < G_1$ and $g > G_1$ are possible. A patient reader can verify, for example, that $g < G_1$ for the pair (11, 17) and $g > G_1$ for the pair (29, 103).

8. The lower bound. It remains to prove that G_2 is a universal lower bound on the Frobenius number, and that it is sharp if $p = 3$ or if (p, q) is a twin prime pair.

PROPOSITION 8.1. *G_2 is not representable for any pair with $\kappa + \lambda < p$.*

Proof. Suppose (p, q) is a pair for which G_2 is representable. Using Proposition 5.3 with $(x_0, y_0, z_0, w_0) = (p' - 1,\ p - 1,\ \kappa, 2 - p)$, there exists an integer l such that

$$\begin{cases} (p'-1)p + p' - lq' = xp + (y+w)p', \\ \kappa p + 2 - p + lq = zp + w, \end{cases} \tag{8.1}$$

for non-negative integers x, y, z, w. The second equation implies $l \ge 0$. Collecting the multiples of p and p' on the left-hand side of the first equation, and using (5.4) and (5.5) with $\kappa = \kappa'$, and Lemma 5.2, we see that there exists $t \in \mathbb{Z}$ such that

$$x = p' - 1 - l\lambda' + tp', \tag{8.2}$$

$$y + w = 1 + l(\lambda - 1) - tp. \tag{8.3}$$

Equation (8.2) implies $t \ge 0$. Putting $q = \kappa p + \lambda$ into the second equation of (8.1),

$$p(\kappa(l+1) - 1) + l\lambda + 2 = zp + w. \tag{8.4}$$

It follows that $w \equiv l\lambda + 2 \pmod{p}$, and, using (8.3), that $y \equiv -(l+1) \pmod{p}$. Hence, there exist $\mu, \nu \in \mathbb{Z}$ such that

$$\begin{aligned} y &= \nu p - (l+1) \qquad (\nu > 0), \\ w &= \mu p + l\lambda + 2. \end{aligned} \tag{8.5}$$

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

By (8.3), $\mu = -t + \nu$. From (8.4), $z = \kappa(l+1) - 1 + t + \nu$.

Thus, a quadruple representing G_2 has the general form

$$\begin{aligned} x &= p' - 1 - l\lambda' + tp' \qquad (t, l \geq 0), \\ y &= \nu p - (l+1) \qquad\quad (\nu > 0), \\ z &= \kappa(l+1) - 1 + t + \nu, \\ w &= -(t+\nu)p + l\lambda + 2. \end{aligned} \tag{8.6}$$

($t = l = 0$, $\nu = 1$ yields the defining representation of G_2.) The requirements $x \geq 0$ and $w \geq 0$ imply

$$\frac{(t+\nu)p - 2}{\lambda} \leq l \leq \frac{(t+1)p' - 1}{\lambda'}.$$

We show that this leads to a contradiction. Minimising the left-hand member of the inequality by taking $\nu = 1$, we obtain

$$\frac{(t+1)p - 2}{\lambda} \leq \frac{(t+1)p' - 1}{\lambda'}. \tag{8.7}$$

Since $\kappa + \lambda < p$, $\lambda' = (\lambda + (\kappa - 1))/2 \geq \lambda/2$, and hence $1/\lambda' \leq 2/\lambda$, with equality if and only if $\kappa = 1$. Rearranging (8.7), we obtain

$$(t+1)\left(\frac{p}{\lambda} - \frac{p'}{\lambda'}\right) \leq \left(\frac{2}{\lambda} - \frac{1}{\lambda'}\right),$$

which is a contradiction if $\kappa = 1$, because the left-hand side is positive (Lemma 7.2(iii)), while the right-hand side is 0. Hence, assume $\kappa > 1$, and multiply both sides by $\lambda\lambda' > 0$. This yields

$$(t+1)(p\lambda' - p'\lambda) \leq 2\lambda' - \lambda.$$

The right-hand side is equal to $\kappa - 1 > 0$, and the left-hand side can be rewritten as

$$\frac{1}{2}(t+1)(p(\kappa + \lambda - 1) - (p-1)\lambda),$$

which simplifies to

$$\frac{1}{2}(t+1)(p(\kappa - 1) + \lambda).$$

Thus, we have

$$\frac{1}{2}(t+1)(p(\kappa - 1)) < \kappa - 1.$$

Cancelling the non-zero factor $\kappa - 1$ leads to the contradiction

$$(t+1)p < 2.$$

□

Thus, $G_2 \leq g$ for all pairs. The bound is attained if $p = 3$, by Theorem 2.1(iii). The next proposition shows that the bound is also attained for twin prime pairs.

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

PROPOSITION 8.2. *If (p, q) is a twin prime pair, all integers $> G_2$ are representable.*

Proof. We adapt the proof of Proposition 4.1 (cf. Proposition 6.1). It suffices to show that the integers in the closed interval $[G_2 + 1, G_2 + d_1]$ are representable. We start with the representation $G_2 + 1 = \mathfrak{f}(0, p - 1, 0, 0)$, obtained from (4.7) by subtracting $p - 3$ from the fourth coordinate, and using the fact that $\kappa = 1$. For twin pairs, $q' = p' + 1$ and hence, from (4.4) and (4.5), we derive

$$\mathfrak{f}(0, -1, 1, 0) = 1. \tag{8.8}$$

Let an integer $t \in [0, d_1 - 1]$ be represented with the division algorithm as

$$t = aq' + b + c, \quad \text{with} \quad 0 \le a \le p - 1 \ (a \ \text{maximal}), \quad b, c \ge 0, \quad b + c \le p'.$$

The bound on $b + c$ comes from the maximality of a and the fact that $q' = p' + 1$. a and $b + c$ are uniquely determined by t and conversely. It follows from (4.4), (4.6) and (8.8) that, for $t \in [0, d_1 - 1]$,

$$G_2 + 1 + t = \mathfrak{f}(0, p - 1, 0, 0) + a \cdot \mathfrak{f}(0, -1, 0, 1) + b \cdot \mathfrak{f}(0, -1, 1, 0) + c \cdot \mathfrak{f}(1, 0, 0, -2).$$

Thus $G_2 + 1 + t = \mathfrak{f}(x, y, z, w)$, where

$$\begin{aligned} x &= c \\ y &= p - 1 - (a + b) \\ z &= b \\ w &= a - 2c. \end{aligned}$$

If $a \le p'$, then $p - 1 - a \ge p'$ and we may assume $c = 0$ by increasing b, if necessary, while maintaining $y \ge 0$. In fact, $y \ge p - 1 - (p' + p') = 0$, $w = a \ge 0$, and we have a non-negative quadruple. Hence suppose $a = p' + s$, $1 \le s \le p'$. Let $b = p' - i$ and $c = p' - k$, $0 \le i, k \le p'$. Since $b + c \le p'$, $i + k \ge p'$. We claim there is a choice of i and k making (x, y, z, w) a non-negative quadruple. Clearly $x, z \ge 0$ for all choices of i, k. If $i \ge s$, $w = s + 2k - p' \ge i + k + k - p' \ge p' + k - p' = k \ge 0$. If $i < s$, put $i' = i + (s - i) = s$ and $k' = k - (s - i)$, so that $i' + k' = i + k \ge p'$. Let $b = p' - i'$ and $c = p' - k'$. Then

$$\begin{aligned} x &= p' - k' > p' - k \ge 0 \\ y &= i' - s = 0 \\ z &= p' - i' = p' - s \ge 0 \\ w &= i' + 2k' - p' \\ &= i' + k' + k' - p' \\ &\ge p' + k' - p' = k' \ge 0. \end{aligned}$$

□

REMARK 2. We conjecture that $g = G_2$ only if (p, q) is a twin prime pair.

This completes the proofs of Theorems 2.1, 2.3 and 2.4.

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

9. The largest non-genus of $\mathbb{Z}_{pq}$. We return to the motivating question of determining the largest non-genus ν_{pq} of a $\mathbb{Z}_{pq}$ action (Problem II, Section 3.1, $n = pq$). We show that given $p > 3$, the lower bound in (1.4) (and (3.6)) is attained for all but finitely many $q > p$. This is Theorem 2.5 which we restate here.

THEOREM 9.1. *For primes $3 < p < q$, with $\kappa + \lambda \geq p$ and $q \neq 2p - 1, 3p - 2$, the largest non-genus of $\mathbb{Z}_{pq}$ is*

$$\nu_{pq} = G_0 - pq + 1,$$

where G_0 is the integer defined at (2.4)*, equal to the Frobenius number $g(\{d_0, d_1, d_2, d_3\})$.*

Proof. We re-visit the argument in Section 4, showing that the quadruples constructed there satisfy the admissibility conditions required by Lemma 3.2, or can be altered (by adding integer linear combinations of the vectors e_0, e_1, e_2), so as to satisfy them. Bringing the notation in Lemma 3.2 into accord with that introduced in Sections 1 and 2, we put $p = p_1$, $q = p_2$, and use x, y, z, w and d_0, d_1, d_2, d_3 instead of $x_{00}, x_{10}, x_{01}, x_{11}$, and $d_{00}, d_{10}, d_{01}, d_{11}$, respectively. In this notation, conditions (3.4) and (3.5) are

$$y + w \neq 1, \qquad z + w \neq 1, \tag{9.1}$$

$$x + y + w \neq 0, \qquad x + z + w \neq 0. \tag{9.2}$$

It is convenient to replace the condition $y + w \neq 1$ with the stronger condition $y + w > 1$. A non-negative quadruple satisfying (9.1), (9.2) and $y + w \neq 0$ will be called *strongly admissible*. The extra condition is imposed so that if (x, y, z, w) is strongly admissible, then $(x, y + 1, z, w)$ is admissible. With this guarantee, it is sufficient to produce strongly admissible representations of the integers in the closed interval $[G_0 + 1, G_0 + d_1]$.

Suppose first that the quadruple (x, y, z, w) as defined by (4.9) - (4.12) is non-negative, that is, assume $z \geq 0$. One easily verifies that $x + y + w \geq p - 1 > 0$, $x + z + w \geq \kappa > 0$, $y + w \geq p - 1 > 1$. It remains to consider the possibility that

$$z + w = \kappa - 1 - b + p - 3 - 2c + a + b = 1.$$

This occurs if and only if

(i) $\kappa = 1$ and $(a, b, c) = (1, b, p' - 1)$; or
(ii) $\kappa = 2$ and $(a, b, c) = (0, b, p' - 1)$.

$b \leq \kappa - 1$ by (4.11) and the assumption $z \geq 0$. Thus in (i), $b = 0$. The triple $(1, 0, p' - 1)$ corresponds to the inadmissible quadruple $(p' - 1, p - 2, 0, 1)$. $\kappa = 1$ is equivalent to $p + 2 \leq q \leq 2p - 1$ or $q' \leq 2p'$. We have excluded $q = 2p - 1$, so we may assume $q' < 2p'$. It is easily verified that $(p' - 1, p - 2, 0, 1) + e(0, 0)$ is strongly admissible. In case (ii), $b = 0$ or 1 and the two triples $(0, 0, p' - 1)$ and $(0, 1, p' - 1)$ correspond to the inadmissible quadruples

$$(p' - 1, p - 1, 1, 0) \quad \text{and} \quad (p' - 1, p - 1, 0, 1), \tag{9.3}$$

respectively. $\kappa = 2$ is equivalent to $2p + 1 \leq q \leq 3p - 2$ or $p \leq q' \leq 3p'$. Since we have excluded $q = 3p - 2$, we may assume $q' < 3p'$. Addition of $e(0, 1)$ makes both quadruples in (9.3) strongly admissible.

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

Now assume that $z < 0$ in the quadruple (x, y, z, w) defined at (4.9)-(4.12). We re-visit the proofs of Lemmas 4.3, 4.4 and 4.5.

If $s < \kappa' - \kappa - 1$, Lemma 4.3(ii) produces the non-negative quadruple

$$\begin{aligned} x' &= c + (s+1)p', \\ y' &= p - 1 - a, \\ z' &= 0, \\ w' &= p - 3 - 2c + a + \kappa + s - (s+1)p. \end{aligned}$$

If this is inadmissible, $w' \leq 1$. By (4.13) and Lemma 4.3(i), w' is the sum of three non-negative quantities: $(p - 3 - 2c)$, a and $\kappa + s - (s+1)p$. Since $p - 3 - 2c$ is even, $w' \leq 1$ implies $p - 3 - 2c = 0$, equivalently, $c = p' - 1$. The other two quantities are either both 0, or one is 0 and the other is 1. This yields three possible quadruples: $(x',\ p-1,\ 0, 0)$, which is strongly admissible, and

$$(x', p - 1 - a, 0, 1), \quad a = 0, 1, \tag{9.4}$$

where $x' = p' - 1 + (s+1)p'$. We show that these two quadruples cannot arise under the assumed conditions. They are supposed to represent the integers

$$G_0 + aq' + (\kappa + s)p' + p' - 1, \quad a = 0, 1.$$

Equating these two integers with the corresponding values of $\mathfrak{f}$ on the two quadruples in (9.4), we obtain, for $a = 0, 1$,

$$\mathfrak{f}(p' - 1, p - 1, \kappa, -1) + aq' + (\kappa + s)p' + p' - 1 = \mathfrak{f}(p' - 1 + (s+1)p', p - 1 - a, 0, 1).$$

By the linearity of $\mathfrak{f}$ this is equivalent to

$$\begin{aligned} 0 &= \mathfrak{f}(-(s+1)p', a, \kappa, -2) + aq' + (\kappa + s)p' + p' - 1 \\ &= -(s+1)p'd_0 + a(d_1 + q') + \kappa(d_2 + p') - 2d_3 + (s+1)p' - 1 \\ &= -(s+1)p'(d_0 - 1) + a(d_1 + q') + \kappa(d_2 + p') - 2d_3 - 1. \end{aligned} \tag{9.5}$$

The identities

$$d_1 + q' = d_2 + p' = d_3 \quad \text{and} \quad 2d_3 + 1 = d_0 \tag{9.6}$$

follow easily from the d_i definitions in (1.2). Thus (9.5) is equivalent to

$$\begin{aligned} d_0 &= -(s+1)p'(2d_3) + (a + \kappa)d_3 \\ &= (a + \kappa - 2p'(s+1))d_3 \\ &= (a + \kappa - (p-1)(s+1))d_3 \\ &= (a + \kappa + s - (s+1)p + 1)d_3. \end{aligned} \tag{9.7}$$

The expression in parentheses on the right is equal to $w' + 1 = 2$. Thus (9.7) is equivalent to $d_0 = 2d_3$, contradicting the last identity in (9.6).

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

If $s = \kappa' - \kappa - 1$, Lemma 4.4(ii) produces the non-negative quadruple

$$\begin{aligned} x' &= c - \lambda', \\ y' &= p - 2 - a, \\ z' &= \kappa, \\ w' &= p - 3 - 2c + a + [\kappa' - 1 - (\kappa' - \kappa)p + \lambda]. \end{aligned} \tag{9.8}$$

We claim that the quantity in brackets in (9.8) is non-negative. This is a consequence of

$$\begin{aligned} q' &\geq \kappa' p', \\ q - 1 &\geq \kappa'(p - 1), \\ \kappa' - 1 &\geq \kappa' p - q \\ &= (\kappa' - \kappa)p + \kappa p - q \\ &= (\kappa' - \kappa)p - \lambda. \end{aligned} \tag{9.9}$$

It follows that (9.8) is the sum of the three non-negative quantities $(p - 3 - 2c)$, a, and $\kappa' - 1 - (\kappa' - \kappa)p + \lambda$. If the quadruple is inadmissible, $w' \leq 1$ and hence the even number $p - 3 - 2c = 0$, or equivalently, $c = p' - 1$. The other two quantities are either both 0, or one of them is 1 and the other is 0. If $\kappa' - 1 - (\kappa' - \kappa)p + \lambda = 1$, then $a = 0$, and we have the strongly admissible quadruple $(p' - 1 - \lambda', p - 2, \kappa, 1)$. If $\kappa' - 1 - (\kappa' - \kappa)p + \lambda = 0$, then reversing the chain of inequalities ending at (9.9), with inequalities replaced by equalities, $q' = \kappa' p'$. In that case, $\lambda' = 0$ and we have the quadruples

$$(p' - 1,\ p - 2 - a,\ \kappa,\ 0), \quad a = 0, 1, \tag{9.10}$$

which are strongly admissible if $\kappa > 1$ ($p > 3$ is required here). If $\kappa = 1$, the quadruples in (9.10) are inadmissible, but $\kappa + \lambda \geq p$ implies $\lambda = p - 1$ and $q = 2p - 1$, which is excluded.

If $s = \kappa' - \kappa$, then Lemma 4.5 produces the non-negative quadruple (4.19)–(4.22). If this is inadmissible, $w' \leq 1$. By (4.18), w' is the sum of two non-negative quantities, $2(\lambda' - c) - 2$ and a. Since the former is even, it must be 0. Equivalently, $c = \lambda' - 1$. Hence, there are two quadruples corresponding to $a = 0, 1$:

$$(p' - 1,\ p - 2,\ \kappa,\ 0), \quad (p' - 1,\ p - 3,\ \kappa,\ 1). \tag{9.11}$$

The latter is strongly admissible ($p > 3$ is required) as is the former if $\kappa > 1$. If $\kappa = 1$ $(p' - 1, p - 2, \kappa, 0)$ is inadmissible. Then $q' \leq 2p'$, and, in fact, $q' < 2p'$ since $q \neq 2p - 1$. In that case, addition of $e(0, 0)$ yields a strongly admissible quadruple. This concludes the proof of Theorem 9.1. □

For a twin prime pair, it is not difficult to show that the integer $\mathfrak{f}(0, p - 1, 1, 0)$ has no other non-negative representation, and hence no admissible representation. A straightforward argument, similar to the proof of Proposition 8.2, shows that all the next d_1 integers have strongly admissible representations. This yields the following theorem, whose proof is omitted.

https://doi.org/10.1017/S0017089511000097 Published online by Cambridge University Press

THEOREM 9.2. *For a twin prime pair* (p, q)*,* $p > 3$*, the largest non-genus of* $\mathbb{Z}_{pq}$ *is*

$$v_{pq} = \mathfrak{f}(0, p-1, 1, 0) - pq + 1 = G_2 + 1 + d_2 - pq + 1.$$

Hence, for twin prime pairs, v_{pq} is about midway between the bounds of (1.4).

REFERENCES

1. T. Breuer, *Characters and automorphism groups of compact Riemann surfaces* (Cambridge University Press, Cambridge, UK, 2001).

2. F. Curtis, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand.* **67** (1990), 190–192.

3. H. M. Farkas and I. Kra, *Riemann surfaces*, 2nd edn. (Graduate Texts in Mathematics 71) (Springer-Verlag, New York, NY, 1980).

4. L. Greenberg, Finiteness theorems for Fuchsian and Kleinian groups, in *Discrete groups and automorphic functions* (Harvey W. J., Editor) (Academic Press, London, 1977).

5. M. Hall, *The theory of groups*, 2nd edn. (Chelsea Publishing Company, New York, NY, 1976).

6. R. S. Kulkarni, Symmetries of surfaces, *Topology* **26** (1987) 195–203.

7. R. S. Kulkarni and C. Maclachlan, Cyclic p-groups of symmetries of surfaces, *Glasgow Math. J.* **33** (1991) 213–221.

8. C. Maclachlan and A. Miller, Generating functions for finite group actions on surfaces, *Math. Proc. Camb. Phil. Soc.* **124**(1) (1998) 21–49.

9. R. Miranda, *Algebraic curves and Riemann surfaces* (Graduate Studies in Mathematics 5) (American Mathematical Society, Providence, RI, 1995).

10. J. L. Ramirez-Alfonsin, Complexity of the Frobenius problem, *Combinatorica* **16**(1) (1996) 143–147.

11. J. L. Ramirez-Alfonsin, *The diophantine Frobenius problem* (Oxford Lecture Series in Mathematics and its Applications 30) (Oxford University Press, Oxford, UK, 2005).

12. J. J. Sylvester, Problem 7382, *Educ. Times* **37** (1884) 21.

13. A. Weaver, Genus spectra for split metacyclic groups, *Glasgow Math J.* **43** (2001) 209–218.