Enumeration of I-Graphs: Burnside Does It Again

Marko Petkovšek
Faculty of Mathematics and Physics
University of Ljubljana, Slovenia

Helena Zakrajšek
Faculty of Mechanical Engineering
University of Ljubljana, Slovenia

Abstract

We give explicit and efficiently computable formulas for the number of isomorphism classes of I-graphs, connected I-graphs, bipartite connected I-graphs, generalized Petersen graphs, and bipartite generalized Petersen graphs. The tool that we use is the well-known Cauchy-Frobenius-Burnside lemma.

1 Introduction

Recently the class of I-graphs, introduced in the Foster Census [2] as a further development of the generalized Petersen graphs, has received considerable attention. One reason for this is that bipartite I-graphs give rise to some highly symmetric configurations of points and lines [1]. In the same paper, Boben, Pisanski and Žitnik characterized the automorphism groups of those I-graphs which are not generalized Petersen graphs, so that together with the earlier results of Frucht, Graver and Watkins [3], the characterization of the automorphism groups of I-graphs is now complete. Finally, Horvat, Pisanski and Žitnik have recently shown that every I-graph has a nondegenerate unit-distance representation in the Euclidean plane [4]. This answers the question of whether every generalized Petersen graph can be drawn in the plane in such a way that all edges are represented by straight-line segments of equal length.

As witnessed by the recent inclusion of the corresponding counting sequences in [10], there has also been interest in the enumeration of non-isomorphic I-graphs and various of their subclasses, such as connected I-graphs, generalized Petersen graphs, etc. However, explicit formulas for the n-th term of these sequences seem to be unknown, with the sole exception of the formula for the number of non-isomorphic generalized Petersen graphs $G(n,k)$ on $2n$ vertices with $\gcd(n,k)=1$, given quite recently by Steimle and Staton [12, Thm. 11].

At a seminar meeting in Ljubljana in January 2009, T. Pisanski asked for a formula enumerating non-isomorphic I-graphs on $2n$ vertices. We give such a formula below in Section 2, as well as analogous formulas enumerating non-isomorphic connected I-graphs, bipartite connected I-graphs, generalized Petersen graphs, and bipartite generalized Petersen graphs on $2n$ vertices. These formulas are in closed form, and can be used for efficient computation of the number of isomorphism classes, provided that the prime factorization of n is known.

To enumerate isomorphism classes we use the Cauchy-Frobenius lemma, also known as Burnside's lemma. Although very well known, this lemma is seldom applied directly, but rather indirectly via the Redfield-Pólya enumeration theorem whose proof relies on it. Recently, though, it has been used successfully on its own in several cases (cf. [9, 6, 7]).

For $n \in \mathbb{N}$ write $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ and $\mathbb{Z}'_n = \mathbb{Z}_n \setminus \{0, n/2\}$. Let $n \in \mathbb{N}$, $n \geq 3$, and $j,k \in \mathbb{Z}'_n$. The *I-graph* $I(n,j,k)$ is the graph $G=(V,E)$ where

$$\begin{aligned} V &= \mathbb{Z}_n \times \mathbb{Z}_2, \\ E &= \bigcup_{i=0}^{n-1} \{\{(i,0),(i,1)\},\{(i,0),(i+j,0)\},\{(i,1),(i+k,1)\}\}, \end{aligned}$$

and addition is performed modulo n. Well-known special cases include the n-prism $Y_n = I(n,1,1)$, the Petersen graph $I(5,1,2)$, and the generalized Petersen graph $G(n,k) = I(n,1,k)$, introduced by Watkins in [13].

The I-graph $I(n,j,k)$ is a cubic graph on $2n$ vertices. In [1], several graph-theoretic properties of $I(n,j,k)$ such as connectedness, girth, being bipartite or being vertex-symmetric, are characterized in terms of number-theoretic properties of parameters n, j, k. An algorithm for deciding which sets of parameter values give rise to isomorphic I-graphs is also given there. In [5], the following result (crucial for our enumeration) is proved:

Theorem 1.1 *$I(n,j,k)$ and $I(n,j',k')$ are isomorphic if and only if there exists an integer a, relatively prime to n, such that either $\{j',k'\} = \{aj \bmod n, ak \bmod n\}$ or $\{j',k'\} = \{aj \bmod n, -ak \bmod n\}$.*

We also rely on the following results from [1]:

Theorem 1.2 *The graph $I(n,j,k)$ is connected if and only if $\gcd(n,j,k)=1$.*

Theorem 1.3 *A connected graph $I(n,j,k)$ is bipartite if and only if n is even and j and k are odd.*

In the rest of the paper, we use the following notation (for $n \in \mathbb{N}$):

$$\begin{aligned}
I(n) &= \text{the number of isomorphism classes of I-graphs } I(n,j,k) \\ &\quad \text{(sequence A153846 in [10])} \\
I_c(n) &= \text{the number of isomorphism classes of connected I-graphs} \\ &\quad I(n,j,k) \text{ (sequence A153847 in [10])} \\
I_{bc}(n) &= \text{the number of isomorphism classes of bipartite connected} \\ &\quad \text{I-graphs } I(n,j,k) \\
P(n) &= \text{the number of isomorphism classes of generalized Petersen} \\ &\quad \text{graphs } G(n,k) = I(n,1,k) \text{ (sequence A077105 in [10])} \\
P_b(n) &= \text{the number of isomorphism classes of bipartite generalized} \\ &\quad \text{Petersen graphs } G(n,k) = I(n,1,k) \text{ (sequence A107452 in [10])} \\
P_r(n) &= \text{the number of isomorphism classes of generalized Petersen} \\ &\quad \text{graphs } G(n,k) = I(n,1,k) \text{ with } \gcd(n,k) = 1
\end{aligned}$$

$$\begin{aligned}
\mathbb{Z}_n &= \{0,1,\ldots,n-1\} && \text{(the ring of integers modulo } n) \\
\mathbb{Z}_n^* &= \{a \in \mathbb{Z}_n;\ \gcd(a,n) = 1\} && \text{(the group of units of } \mathbb{Z}_n) \\
\mathbb{Z}_n' &= \mathbb{Z}_n \setminus \{0, n/2\} && \text{(the set of legal values for } j,k \text{ in } I(n,j,k))
\end{aligned}$$

For $k \in \mathbb{Z}$, we write $k \bmod n$ to denote the unique $r \in \mathbb{Z}_n$ such that $k \equiv r \pmod{n}$. In particular, if n is even, then

$$(n/2) \bmod 2 \;=\; \begin{cases} 0, & n \equiv 0 \pmod{4}, \\ 1, & n \equiv 2 \pmod{4}. \end{cases}$$

Table 1 lists the arithmetical functions that appear in the rest of the paper. The column "OEIS id" in Table 1 gives the corresponding identifier from [10].

notation	OEIS id	comments
$\mu(n)$	A008683	Moebius function
$\tau(n)$	A000005	the number of divisors of n
$\varphi(n)$	A000010	Euler's totient function, $\varphi(n) = \lvert\{j \in \mathbb{Z}_n;\ \gcd(n,j) = 1\}\rvert = \lvert\mathbb{Z}_n^*\rvert$
$J_2(n)$	A007434	the second Jordan's totient function, $J_2(n) = \lvert\{(j,k) \in \mathbb{Z}_n \times \mathbb{Z}_n;\ \gcd(n,j,k) = 1\}\rvert$
$\omega(n)$	A001221	the number of distinct prime factors of n
$r(n)$	A060594	the number of square roots of 1 modulo n, $r(n) = \lvert\{a \in \mathbb{Z}_n;\ a^2 \equiv 1 \pmod{n}\}\rvert$
$s(n)$	A000089	the number of square roots of -1 modulo n, $s(n) = \lvert\{a \in \mathbb{Z}_n;\ a^2 \equiv -1 \pmod{n}\}\rvert$

Table 1: Some arithmetical functions

With the exception of $\omega(n)$ which is additive, all other functions in Table 1 are multiplicative. If p is a prime and $k \geq 1$, we have

$$J_2(p^k) \;=\; p^{2k} - p^{2k-2} \;=\; \sum_{d\,|\,p^k} \mu\left(\frac{p^k}{d}\right) d^2,$$

$$r(p^k) \;=\; \begin{cases} 1, & p = 2 \text{ and } k = 1, \\ 2, & p \text{ odd} \quad \text{or} \quad (p = 2 \text{ and } k = 2), \\ 4, & p = 2 \text{ and } k \geq 3, \end{cases}$$

$$s(p^k) \;=\; \begin{cases} 0, & p \equiv 3 \pmod 4 \quad \text{or} \quad (p = 2 \text{ and } k \geq 2), \\ 1, & p = 2 \text{ and } k = 1, \\ 2, & p \equiv 1 \pmod 4, \end{cases}$$

hence

$$J_2(n) \;=\; n^2 \prod_{\substack{p\,|\,n \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right) \;=\; \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) d^2,$$

$$r(n) \;=\; \begin{cases} 2^{\omega(n)}, & n \equiv 1 \pmod 2 \quad \text{or} \quad n \equiv 4 \pmod 8, \\ 2^{\omega(n)-1}, & n \equiv 2 \pmod 4, \\ 2^{\omega(n)+1}, & n \equiv 0 \pmod 8, \end{cases}$$

$$s(n) \;=\; \begin{cases} 0, & 4\,|\,n \quad \text{or} \quad \exists p \text{ prime} : (p\,|\,n \text{ and } p \equiv 3 \pmod 4), \\ 2^{\psi(n)}, & \text{otherwise}, \end{cases}$$

where $\psi(n) = |\{p\,|\,n;\; p \text{ prime}, p \equiv 1 \,(\text{mod } 4)\}|$.

The following formula (which can also be proved by our methods) is given in [12, Thm. 11]:

Theorem 1.4 *The number $P_r(n)$ of isomorphism classes of generalized Petersen graphs $G(n, k)$ on $2n$ vertices with $\gcd(n, k) = 1$ is given by*

$$P_r(n) \;=\; \frac{1}{4}(\varphi(n) + r(n) + s(n)). \tag{1}$$

In Section 2 we list our formulas for $I(n)$, $I_c(n)$, $I_{bc}(n)$, $P(n)$, $P_b(n)$ which seem to be new, and tabulate their values (as well as those of $P_r(n)$) for some small values of n. In Section 3 we explain our proof techniques and give the proofs.

2 The main results

Theorem 2.1 *Let $n = p_1^{k_1} p_2^{k_2} \cdots p_{\omega(n)}^{k_{\omega(n)}}$ be the prime factorization of n. Then the number of isomorphism classes of I-graphs on $2n$ vertices is given by*

$$I(n) \;=\; \frac{1}{4} \sum_{i=1}^{4} \prod_{j=1}^{\omega(n)} g_i\left(p_j^{k_j}\right) - \begin{cases} 2\tau(n) - 1, & n \text{ even}, \\ \tau(n), & n \text{ odd}, \end{cases} \tag{2}$$

where

$$g_1(p^k) \;=\; \frac{(p+1)p^k-2}{p-1}, \tag{3}$$

$$g_2(p^k) \;=\; \begin{cases} 4k, & p=2, \\ 2k+1, & p>2, \end{cases} \tag{4}$$

$$g_3(p^k) \;=\; \begin{cases} 2, & p=2 \textit{ and } k=1, \\ 4(k-1), & p=2 \textit{ and } k\geq 2, \\ 2k+1, & p>2, \end{cases} \tag{5}$$

$$g_4(p^k) \;=\; \begin{cases} 2, & p=2, \\ 2k+1, & p\equiv 1 \pmod 4, \\ 1, & p\equiv 3 \pmod 4. \end{cases} \tag{6}$$

Theorem 2.2 *The number $P(n)$ of isomorphism classes of generalized Petersen graphs on $2n$ vertices is given by*

$$P(n) \;=\; \frac{1}{4}(2n-\varphi(n)-2\gcd(n,2)+r(n)+s(n)). \tag{7}$$

Theorem 2.3 *The number of isomorphism classes of connected I-graphs on $2n$ vertices is given by*

$$I_c(n) \;=\; \frac{1}{4}\left(\frac{J_2(n)}{\varphi(n)}+r(n)+s(n)+t(n)\right)-\begin{cases} 1, & n \text{ odd}, \\ 2, & n\equiv 0 \pmod 4, \\ 3, & n\equiv 2 \pmod 4) \end{cases} \tag{8}$$

where

$$t(n) \;=\; \begin{cases} 2^{\omega(n)}+2^{\omega(n/2)}, & n \text{ even}, \\ 2^{\omega(n)}, & n \text{ odd}. \end{cases} \tag{9}$$

Theorem 2.4 *For n even, let $\chi(n)=(n/2) \bmod 2$. The number of isomorphism classes of bipartite generalized Petersen graphs on $2n$ vertices is given by*

$$P_b(n)=\begin{cases} \frac{1}{4}\left(n-\varphi(n)-2\chi(n)+r(n)+s(n)\right), & n \text{ even} \\ 0, & n \text{ odd}. \end{cases} \tag{10}$$

Theorem 2.5 *For n even, let $\chi(n)=(n/2) \bmod 2$. The number of isomorphism classes of bipartite connected I-graphs on $2n$ vertices is given by*

$$I_{bc}(n) \;=\; \begin{cases} \frac{1}{4}\left(\frac{J_2(n)}{3\varphi(n)}+\chi(n)\,2^{\omega(n/2)}+r(n)+s(n)\right)-\chi(n), & n \text{ even} \\ 0, & n \text{ odd}. \end{cases} \tag{11}$$

Corollary 2.6 *Let p be an odd prime. Then*

$$I(p) \;=\; I_c(p) \;=\; P(p) \;=\; P_r(p) \;=\; \left\lceil \frac{p}{4} \right\rceil.$$

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$I(n)$	1	1	2	3	2	4	4	6	3	11	4	7	10	10	5	14	5	17	12
$I_c(n)$	1	1	2	2	2	3	3	4	3	7	4	5	7	6	5	8	5	10	9
$P(n)$	1	1	2	2	2	3	3	4	3	5	4	5	6	6	5	7	5	8	8
$P_r(n)$	1	1	2	1	2	2	2	2	3	2	4	2	3	3	5	2	5	3	4

n	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
$I(n)$	11	6	28	10	14	13	21	8	35	8	22	17	18	17	41	10	19
$I_c(n)$	8	6	14	8	10	9	13	8	19	8	12	13	13	13	19	10	14
$P(n)$	8	6	11	8	10	9	11	8	13	8	12	12	13	12	15	10	14
$P_r(n)$	3	6	4	6	4	5	4	8	3	8	5	6	5	7	4	10	5

n	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55
$I(n)$	20	40	11	44	11	31	32	23	12	60	16	36	25	37	14	49	24
$I_c(n)$	15	20	11	25	11	19	19	17	12	26	14	22	19	22	14	26	19
$P(n)$	14	17	11	18	11	17	17	17	12	21	14	20	18	20	14	22	18
$P_r(n)$	7	6	11	4	11	6	7	6	12	6	11	6	9	7	14	5	11

n	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72
$I(n)$	50	27	30	15	93	16	31	40	46	29	64	17	47	32	63	18	96
$I_c(n)$	26	21	22	15	40	16	23	25	24	23	37	17	28	25	37	18	38
$P(n)$	23	20	22	15	27	16	23	23	24	22	28	17	26	24	29	18	31
$P_r(n)$	8	10	8	15	6	16	8	10	9	14	6	17	9	12	7	18	8

n	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88
$I(n)$	19	38	49	51	30	75	20	84	40	42	21	117	36	43	40	72
$I_c(n)$	19	28	31	31	25	43	20	38	27	31	21	52	29	32	31	38
$P(n)$	19	28	28	29	24	33	20	33	27	31	21	37	28	32	30	35
$P_r(n)$	19	10	11	10	16	7	20	10	14	11	21	8	18	11	15	12

n	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103
$I(n)$	23	120	35	61	42	47	38	122	25	62	57	93	26	95	26
$I_c(n)$	23	55	29	37	33	35	31	50	25	41	37	46	26	55	26
$P(n)$	23	39	28	35	32	35	30	41	25	38	35	40	26	43	26
$P_r(n)$	23	7	19	12	16	12	19	10	25	11	16	11	26	9	26

Table 2: The values of $I(n)$, $I_c(n)$, $P(n)$, $P_r(n)$ for $3 \leq n \leq 103$

n	104	105	106	107	108	109	110	111	112	113	114	115	116
$I(n)$	84	85	54	27	131	28	91	50	106	29	104	45	77
$I_c(n)$	44	51	40	27	55	28	55	39	50	29	61	37	46
$P(n)$	41	42	40	27	45	28	45	38	45	29	48	36	44
$P_r(n)$	14	14	14	27	10	28	11	19	14	29	10	23	15

n	117	118	119	120	121	122	123	124	125	126	127	128	129
$I(n)$	66	59	44	208	36	62	55	81	48	153	32	94	57
$I_c(n)$	43	44	37	78	33	46	43	49	38	73	32	48	45
$P(n)$	41	44	36	55	33	46	42	47	38	54	32	48	44
$P_r(n)$	19	15	25	12	28	16	21	16	26	10	32	17	22

n	130	131	132	133	134	135	136	137	138	139	140	141	142
$I(n)$	108	33	167	48	67	96	106	35	124	35	163	62	71
$I_c(n)$	65	33	76	41	50	55	56	35	73	35	76	49	53
$P(n)$	54	33	57	40	50	50	53	35	58	35	59	48	53
$P_r(n)$	14	33	12	28	17	19	18	35	12	35	14	24	18

Table 3: The values of $I(n)$, $I_c(n)$, $P(n)$, $P_r(n)$ for $105 \le n \le 142$

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
$I_{bc}(n)$	1	1	2	2	3	2	3	3	4	3	6	4	5	7	5	5	7
$P_b(n)$	1	1	2	2	3	2	3	3	4	3	6	4	5	6	5	5	7

n	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66	68
$I_{bc}(n)$	5	8	9	7	6	10	8	8	9	10	8	14	8	9	13	10
$P_b(n)$	5	8	8	7	6	10	8	8	9	10	8	13	8	9	12	10

n	70	72	74	76	78	80	82	84	86	88	90	92	94	96	98	100
$I_{bc}(n)$	13	14	10	11	15	14	11	18	11	14	19	13	12	18	14	16
$P_b(n)$	12	14	10	11	14	14	11	17	11	14	17	13	12	18	14	16

n	102	104	106	108	110	112	114	116	118	120	122	124	126
$I_{bc}(n)$	19	16	14	19	19	18	21	16	15	28	16	17	25
$P_b(n)$	18	16	14	19	18	18	20	16	15	26	16	17	23

n	128	130	132	134	136	138	140	142	144	146	148	150	152
$I_{bc}(n)$	17	23	26	17	20	25	26	18	26	19	20	31	22
$P_b(n)$	17	22	25	17	20	24	25	18	26	19	20	28	22

Table 4: The values of $I_{bc}(2n)$ and $P_b(2n)$ for $2 \le n \le 76$

3 The proofs

3.1 The Burnside technology

Let α be the action of a finite group G on a finite set A. Then we denote by $\sim_\alpha$ the associated equivalence relation on A, by $|A/{\sim_\alpha}|$ the number of orbits of α, and by $\mathrm{fix}_\alpha(g)$ the number of elements of A fixed by $g \in G$ under α. Our main enumeration tool is the *Cauchy-Frobenius-Burnside lemma*:

Lemma 3.1

$$|A/{\sim_\alpha}| \;=\; \frac{1}{|G|}\sum_{g\in G}\mathrm{fix}_\alpha(g).$$

For a proof, see, e.g., [11, Lemma 7.24.5]).

First we list some auxiliary results which will be useful in the sequel.

Proposition 3.2 *Let ϑ_n be the multiplicative action of $\mathbb{Z}_n^*$ on $\mathbb{Z}_n$. Then*

$$|\mathbb{Z}_n/{\sim_{\vartheta_n}}| \;=\; \frac{1}{\varphi(n)}\sum_{a\in\mathbb{Z}_n^*}\gcd(n,a-1). \tag{12}$$

Proof: Assume that $j \in \mathbb{Z}_n$, $a \in \mathbb{Z}_n^*$, $d = \gcd(n, a-1)$, $n = n'd$ and $a - 1 = a'd$. Then $\gcd(n', a') = 1$, and so j is fixed by a iff

$$aj \equiv j \pmod{n} \iff n \,|\, (a-1)j \iff n' \,|\, a'j \iff n' \,|\, j.$$

It follows that the set of j fixed by a is $\{0, n', 2n', \ldots, (d-1)n'\}$, hence $\mathrm{fix}_\vartheta(a) = d = \gcd(n, a-1)$, and Lemma 3.1 gives (12). □

Lemma 3.3 *Let $a, d, n \in \mathbb{N}$ be such that $d \,|\, n$ and $\gcd(a, d) = 1$. Then there is an $x \in \mathbb{Z}$ such that $\gcd(a + xd, n) = 1$.*

Proof: Let $x \in \mathbb{Z}_n$ satisfy

$$x \not\equiv -a\,d^{-1} \pmod{p}$$

for each prime p which divides n but not d. Note that d is invertible mod p for such p, and that such an x exists by the Chinese Remainder Theorem.

Assume that $\gcd(a + xd, n) \neq 1$. Then there exists a prime p such that $p \,|\, n$ and $p \,|\, (a + xd)$. We distinguish two cases.

a) If $p \,|\, d$ then $p \,|\, a$, contrary to the assumption that $\gcd(a, d) = 1$.

b) If $p \not| d$ then

$$a + xd \equiv 0 \pmod{p} \implies x \equiv -a\, d^{-1} \pmod{p},$$

contrary to the choice of x.

In either case we reach a contradiction, hence $\gcd(a + xd, n) = 1$. □

Corollary 3.4 *Let ϑ_n be as in Proposition 3.2. For all $j, k \in \mathbb{Z}_n$ we have:*

(i) $j \sim_{\vartheta_n} \gcd(n, j)$,

(ii) $j \sim_{\vartheta_n} k \iff \gcd(n, j) = \gcd(n, k)$,

(iii) *each orbit of ϑ_n contains exactly one positive divisor of n (with n replaced by 0), and $|\mathbb{Z}_n/{\sim_{\vartheta_n}}| = \tau(n)$.*

Proof: (i) Let $d = \gcd(n, j)$, $n' = n/d$, $j' = j/d$. Then $\gcd(n', j') = 1$, so there are $a', k \in \mathbb{Z}$ such that $a'j' = 1 + kn'$. Since $\gcd(a', n') = 1$ and $n' \mid n$, Lemma 3.3 implies that there is an $x \in \mathbb{Z}$ such that $a := a' + xn' \in \mathbb{Z}_n^*$. Then

$$aj \;=\; (a' + xn')j'd \;=\; a'j'd + xj'n \;=\; (1 + kn')d + xj'n \;=\; d + (k + xj')n,$$

hence $aj \equiv d \pmod{n}$. So $j \sim_{\vartheta_n} d$, proving the claim.

(ii) Let $j \sim_{\vartheta_n} k$. Then there are $a \in \mathbb{Z}_n^*$ and $m \in \mathbb{Z}$ such that $aj - k = mn$. This implies that any common divisor of j and n divides k, and any common divisor of k and n divides aj and hence j. It follows that $\gcd(n, j) = \gcd(n, k)$.

Conversely, let $\gcd(n, j) = \gcd(n, k)$. Then by (i), $j \sim_{\vartheta_n} k$.

(iii) By (i), each orbit of $\sim_{\vartheta_n}$ contains a positive divisor of n (with n replaced by 0). By (ii), different positive divisors of n (with n replaced by 0) belong to different orbits of $\sim_{\vartheta_n}$. This proves the claim. □

Lemma 3.5 *Let $a, b, c \in \mathbb{Z}$, $n, k \in \mathbb{N}$.*

(i) *If* $a \equiv b \pmod{n}$ *then* $\gcd(a, n) = \gcd(b, n)$.

(ii) *If* $\gcd(a, b) = 1$ *then* $\gcd(ab, c) = \gcd(a, c)\gcd(b, c)$.

(iii) *Any set of nk consecutive integers contains exactly k multiples of n.*

The straightforward proofs are omitted.

Now we embark on our main task of enumerating isomorphism classes of I-graphs. For a fixed $n \geq 3$, we represent the I-graph $I(n, j, k)$ with the ordered pair (j, k). We need to construct a suitable group G_n acting on the set $\mathbb{Z}_n \times \mathbb{Z}_n$ in such a way that the orbits of this action will be in one-to-one correspondence with the isomorphism classes of I-graphs. In view of Theorem 1.1, the following choice is natural.

Definition 3.6 *By G_n we denote the subgroup of the symmetric group $S(\mathbb{Z}_n \times \mathbb{Z}_n)$ generated by the permutations $(\xi_a)_{a\in\mathbb{Z}_n^*}, \mu, \rho: \ \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$, where for all $a \in \mathbb{Z}_n^*$ and $(j,k) \in \mathbb{Z}_n \times \mathbb{Z}_n$:*

$$\begin{aligned} \xi_a(j,k) &\equiv (aj, ak) \pmod{n}, \\ \mu(j,k) &\equiv (j, -k) \pmod{n}, \\ \rho(j,k) &\equiv (k, j) \pmod{n}. \end{aligned}$$

Proposition 3.7

$$G_n = \{\xi_a, \xi_a\mu, \xi_a\rho, \xi_a\rho\mu; \ a \in \mathbb{Z}_n^*\} \tag{13}$$

and $|G_n| = 4\varphi(n)$.

Proof: It is straightforward to check that for all $a, b \in \mathbb{Z}_n^*$,

$$\begin{aligned} \xi_a\xi_b &= \xi_{ab}, \\ \xi_a\xi_{a^{-1}} = \xi_1 &= \mathrm{id}_{\mathbb{Z}_n\times\mathbb{Z}_n} = \mu^2 = \rho^2, \\ \mu\xi_a &= \xi_a\mu, \\ \rho\xi_a &= \xi_a\rho, \\ \mu\rho &= \xi_{-1}\rho\mu. \end{aligned}$$

Using these equalities we can show that for any $g \in G_n$ there are $a \in \mathbb{Z}_n^*$ and $\epsilon, \delta \in \{0,1\}$ such that

$$g = \xi_a\rho^\epsilon\mu^\delta,$$

which proves (13). Now write $g_i = \xi_{a_i}\rho^{\epsilon_i}\mu^{\delta_i}$ for $i \in \{1,2\}$. Assume that $g_1 = g_2$, and compute

$$g_i(1,1) = \begin{cases} (a_i, (-1)^{\delta_i}a_i), & \epsilon_i = 0, \\ ((-1)^{\delta_i}a_i, a_i), & \epsilon_i = 1. \end{cases}$$

If $\epsilon_1 \neq \epsilon_2$, then $g_1(1,1) = g_2(1,1)$ implies that $a_1 = (-1)^{\delta_2}a_2$ and $a_2 = (-1)^{\delta_1}a_1$, hence $a_1 = (-1)^{\delta_1+\delta_2}a_1$. Cancelling a_1 yields $(-1)^{\delta_1+\delta_2} = 1$, and so $\delta_1 = \delta_2$. W.l.g. assume that $\epsilon_1 = 1$ and $\epsilon_2 = 0$. Then $g_1 = g_2$ turns into $\xi_{a_1}\rho = \xi_{a_2}$. Applying both sides of this equality to $(1,1)$ yields $(a_1, a_1) = (a_2, a_2)$, hence $a_1 = a_2$ and $\xi_{a_1} = \xi_{a_2}$. Now $\xi_{a_1}\rho = \xi_{a_2}$ implies $\rho = \xi_1$. On the other hand, the initial assumption that $n \geq 3$ implies that $|\mathbb{Z}_n^*| \geq 2$, hence $\rho \neq \xi_1$.

This contradiction shows that $\epsilon_1 = \epsilon_2$. Then $g_1(1,1) = g_2(1,1)$ implies that $a_1 = a_2$ and $(-1)^{\delta_1}a_1 = (-1)^{\delta_2}a_2$, hence $(-1)^{\delta_1} = (-1)^{\delta_2}$, and so $\delta_1 = \delta_2$.

We have shown that $g_1 = g_2$ if and only if $a_1 = a_2$ and $\epsilon_1 = \epsilon_2$ and $\delta_1 = \delta_2$. Hence $|G_n| = 4|\mathbb{Z}_n^*| = 4\varphi(n)$ as claimed. □

Remark 3.8 *Let* $\langle \rho, \mu \rangle$ *be the subgroup of* G_n *generated by* ρ *and* μ. *One can see that* $\langle \rho, \mu \rangle = \{\xi_1,\ \rho,\ \mu,\ \rho\mu,\ \xi_{-1},\ \xi_{-1}\rho,\ \xi_{-1}\mu,\ \xi_{-1}\rho\mu\}$ *is isomorphic to the dihedral group* $D_4 = \langle r, s \mid r^4 = f^2 = (rf)^2 = 1\rangle$, *with* r *corresponding to* $\rho\mu$ *or* $\mu\rho$, *and* f *corresponding to any of* ρ, μ, $\rho\mu\rho$, *or* $\mu\rho\mu$. *The mapping* $h: \mathbb{Z}_n^* \times D_4 \to G_n$ *defined by*

$$h(a, r^i f^j) \;=\; \xi_a (\rho\mu)^i \rho^j, \quad \text{for } i \in \{0,1,2,3\},\ j \in \{0,1\},$$

is a group epimorphism with kernel $C_2 = \langle(-1, r^2)\rangle$, *hence by the first isomorphism theorem for groups,* $G_n \simeq (\mathbb{Z}_n^* \times D_4)/C_2$.

The elements of G_n are permutations of $\mathbb{Z}_n \times \mathbb{Z}_n$, hence the group G_n acts naturally on $\mathbb{Z}_n \times \mathbb{Z}_n$. We denote this action by α_n. In the next lemma we show how to count the isomorphism classes in a set $\mathcal{K}_n$ of I-graphs on $2n$ vertices, by counting the orbits of α_n on an appropriate subset $K_n \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$.

Lemma 3.9 *Let* $\mathcal{K}_n \subseteq \{I(n,j,k);\ j,k \in \mathbb{Z}_n'\}$ *be a set of I-graphs closed under isomorphism. Let* $K_n \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ *satisfy*

$$K_n \cap (\mathbb{Z}_n' \times \mathbb{Z}_n') \;=\; \{(j,k);\ I(n,j,k) \in \mathcal{K}_n\},$$

and $g(K_n) = K_n$ *for all* $g \in G_n$. *Then the restriction of* G_n *to* K_n,

$$G|_{K_n} \;:=\; \{g|_{K_n};\ g \in G_n\},$$

is a subgroup of $S(K_n)$, *so let* $\alpha(K_n)$ *be the action of* $G|_{K_n}$ *on* K_n. *Write*

$$\nu_0(K_n) \;=\; |\{\eta \in K_n/{\sim_{\alpha(K_n)}};\ \eta \not\subseteq \mathbb{Z}_n' \times \mathbb{Z}_n'\}|.$$

Then

$$|\mathcal{K}_n/{\simeq}| \;=\; |K_n/{\sim_{\alpha(K_n)}}| - \nu_0(K_n) \tag{14}$$

where $\simeq$ *denotes graph isomorphism.*

Proof: Write $K_n' = \{(j,k) \in \mathbb{Z}_n' \times \mathbb{Z}_n';\ I(n,j,k) \in \mathcal{K}_n\}$. Note that for any $(j,k), (j',k') \in \mathbb{Z}_n' \times \mathbb{Z}_n'$ we have, by Theorem 1.1 and Proposition 3.7,

$$\begin{aligned}
&I(n,j,k) \;\simeq\; I(n,j',k') \\
&\quad\iff \exists a \in \mathbb{Z}_n^*:\ \{j',k'\} \in \{\{aj, ak\}, \{aj, -ak\}\} \\
&\quad\iff \exists a \in \mathbb{Z}_n^*:\ (j',k') \in \{(aj,ak), (ak,aj), (aj,-ak), (-ak,aj)\} \\
&\quad\iff \exists a \in \mathbb{Z}_n^*:\ (j',k') \in \{\xi_a(j,k), \xi_a\rho(j,k), \xi_a\mu(j,k), \xi_a\rho\mu(j,k)\} \\
&\quad\iff \exists g \in G_n:\ (j',k') = g(j,k)
\end{aligned} \tag{15}$$

where all the arithmetic is done modulo n.

Let $(j, k) \in K'_n$ and $(j', k') = g(j, k)$ for some $g \in G_n$. Then $I(n, j, k) \in \mathcal{K}_n$, and $I(n, j, k) \simeq I(n, j', k')$ by (15), hence $I(n, j', k') \in \mathcal{K}_n$ and $(j', k') \in K'_n$. It follows that $g(K'_n) = K'_n$ for all $g \in G_n$, so $G|_{K'_n}$ is a subgroup of $S(K'_n)$. Let $\alpha(K'_n)$ be the action of $G|_{K'_n}$ on K'_n. By Theorem 1.1, the mapping

$$f : [I(n, j, k)] \mapsto [(j, k)]$$

from $\mathcal{K}_n/\simeq$ to $K'_n/\sim_{\alpha(K'_n)}$ is well defined and injective. Obviously it is also surjective, hence

$$|\mathcal{K}_n/\simeq| = |K'_n/\sim_{\alpha(K'_n)}|. \tag{16}$$

We claim that for any orbit $\eta \in K_n/\sim_{\alpha(K_n)}$, either $\eta \subseteq \mathbb{Z}'_n \times \mathbb{Z}'_n$ or $\eta \subseteq (\mathbb{Z}_n \times \mathbb{Z}_n) \setminus (\mathbb{Z}'_n \times \mathbb{Z}'_n)$. To prove this, assume that $\eta \not\subseteq \mathbb{Z}'_n \times \mathbb{Z}'_n$. Then $(0, k) \in \eta$ or $(n/2, k) \in \eta$ for some $k \in \mathbb{Z}_n$ (the latter only if n is even). Hence for any $(j', k') \in \eta$, there is a $g \in G_n$ such that $(j', k') \in \{g(0, k), g(n/2, k)\}$. From Proposition 3.7 it follows that there are $a, b, c \in \mathbb{Z}^*_n$ such that $\{j', k'\} \in \{\{0, ak\}, \{bn/2, ck\}\}$. If n is even then b is odd, hence $n \mid n(b-1)/2$ and $bn/2 \equiv n/2 \pmod{n}$, implying that $\{j', k'\} \in \{\{0, ak\}, \{n/2, ck\}\}$ for some $a, c \in \mathbb{Z}^*_n$. We conclude that $\eta \subseteq (\mathbb{Z}_n \times \mathbb{Z}_n) \setminus (\mathbb{Z}'_n \times \mathbb{Z}'_n)$ which proves the claim.

It follows that every orbit of $\alpha(K'_n)$ is an orbit of $\alpha(K_n)$, and every orbit of $\alpha(K_n)$ is either an orbit of $\alpha(K'_n)$ or is contained in $(\mathbb{Z}_n \times \mathbb{Z}_n) \setminus (\mathbb{Z}'_n \times \mathbb{Z}'_n)$. Hence

$$|K_n/\sim_{\alpha(K_n)}| = |K'_n/\sim_{\alpha(K'_n)}| + \nu_0(K_n),$$

which, together with (16), completes the proof. □

In the rest of the paper we proceed as follows. For each of the (five) sets $\mathcal{K}_n$ of I-graphs whose isomorphism classes we wish to enumerate, we select an appropriate set $K_n \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, and check that the assumptions of Lemma 3.9 are satisfied. Then we count the orbits of $\alpha(K_n)$ by means of Lemma 3.1, which is tantamount to computing the average number of fixed points of the elements $g \in G|_{K_n}$. This is done by counting the fixed points of g in four steps, corresponding to the four possible types of g, namely ξ_a, $\xi_a\mu$, $\xi_a\rho$ and $\xi_a\rho\mu$ (with $a \in \mathbb{Z}^*_n$). Finally we compute $\nu_0(K_n)$ by counting those orbits of $\alpha(K_n)$ that contain an element of the form $(0, k)$ or $(n/2, k)$, and use (14).

To simplify notation, we write G_n for $G|_{K_n}$ and α_n for $\alpha(K_n)$ in the sequel. This causes no confusion, since in each of the five cases considered it is straightforward to verify that $G|_{K_n} \simeq G_n$.

3.2 I-graphs

Let $\mathcal{K}_n$ be the set of all I-graphs on $2n$ vertices, and $K_n := \mathbb{Z}_n \times \mathbb{Z}_n$.

Proposition 3.10

$$|\mathbb{Z}_n \times \mathbb{Z}_n/{\sim_{\alpha_n}}| \;=\; \frac{1}{4\varphi(n)} \sum_{i=1}^{4} \sum_{a \in \mathbb{Z}_n^*} f_i(a,n)$$

where

$$\begin{aligned} f_1(a,n) &= \gcd(n, a-1)^2, \\ f_2(a,n) &= \gcd(n, a-1)\gcd(n, a+1), \\ f_3(a,n) &= \gcd(n, a^2-1), \\ f_4(a,n) &= \gcd(n, a^2+1). \end{aligned}$$

Proof: We use Lemma 3.1. The fixed points of ξ_a are those pairs (j,k) which satisfy $aj \equiv j \pmod{n}$ and $ak \equiv k \pmod{n}$. As in the proof of Proposition 3.2 we see that there are $d = \gcd(n, a-1)$ such j's, and d such k's, hence d^2 such pairs. The number of fixed points of all ξ_a is thus $\sum_{a\in\mathbb{Z}_n^*} f_1(a,n)$.

The fixed points of $\xi_a\mu$ are those pairs (j,k) which satisfy $aj \equiv j \pmod{n}$ and $-ak \equiv k \pmod{n}$. There are $\gcd(n, a-1)$ such j's, and $\gcd(n, a+1)$ such k's, hence the number of fixed points of all $\xi_a\mu$ is $\sum_{a\in\mathbb{Z}_n^*} f_2(a,n)$.

The fixed points of $\xi_a\rho$ are those pairs (j,k) which satisfy $ak \equiv j \pmod{n}$ and $aj \equiv k \pmod{n}$. Hence $a^2k \equiv k \pmod{n}$, and for any such k, we must take $j \equiv ak \pmod{n}$. There are $\gcd(n, a^2-1)$ such k's, hence the number of fixed points of all $\xi_a\rho$ is $\sum_{a\in\mathbb{Z}_n^*} f_3(a,n)$.

The fixed points of $\xi_a\rho\mu$ are those pairs (j,k) which satisfy $-ak \equiv j \pmod{n}$ and $aj \equiv k \pmod{n}$. Hence $-a^2k \equiv k \pmod{n}$, and for any such k, we must take $j \equiv -ak \pmod{n}$. There are $\gcd(n, a^2+1)$ such k's, hence the number of fixed points of all $\xi_a\rho\mu$ is $\sum_{a\in\mathbb{Z}_n^*} f_4(a,n)$.

Since $|G_n| = 4\varphi(n)$, the assertion follows. □

Now we wish to evaluate the sum appearing in Proposition 3.10 in closed form, given the prime factorization of n. We do this by splitting this double sum into four single sums correspondng to $i = 1,2,3,4$, evaluating each of them in the case when n is a prime power, and showing that they are multiplicative.

Lemma 3.11 *For* $i = 1,2,3,4$*, let*

$$g_i(n) \;=\; \frac{1}{\varphi(n)} \sum_{a\in\mathbb{Z}_n^*} f_i(a,n)$$

where $f_i(a,n)$ *are as in Proposition 3.10. If* p *is a prime and* $k \geq 1$*, then* $g_i(p^k)$ *are as given in equations* (3) – (6).

Proof: Let $x, r \in \mathbb{Z}$ with $\gcd(r,p)=1$. Denote

$$\begin{aligned} \nu_p(x) &= \max\{i \in \mathbb{N};\ p^i \,|\, x\}, \\ M_{k,j}^{(r)}(p) &= \{x \in \mathbb{Z}_{p^k}^* - r;\ \nu_p(x) \geq j\},\ \text{for } 1 \leq j \leq k, \\ N_{k,j}^{(r)}(p) &= \{x \in \mathbb{Z}_{p^k}^* - r;\ \nu_p(x) = j\},\ \text{for } 0 \leq j \leq k-1. \end{aligned}$$

The elements of $(\mathbb{Z}_{p^k} \setminus \mathbb{Z}_{p^k}^*) - r$ are not divisible by p, hence it follows for $j \geq 1$ that $M_{k,j}^{(r)}(p) = \{x \in \mathbb{Z}_{p^k} - r;\ \nu_p(x) \geq j\}$. This is the set of all multiples of p^j in a set of p^k consecutive integers, therefore Lemma 3.5 (iii) implies that $|M_{k,j}^{(r)}(p)| = p^{k-j}$ for $1 \leq j \leq k$ and for all r such that $\gcd(r,p)=1$. Consequently

$$\begin{aligned} |N_{k,j}^{(r)}(p)| &= |M_{k,j}^{(r)}(p)| - |M_{k,j+1}^{(r)}(p)| \ = \ p^{k-j} - p^{k-j-1} \quad \text{for } 1 \leq j \leq k-1, \\ |N_{k,0}^{(r)}(p)| &= |\mathbb{Z}_{p^k}^* - r| - |M_{k,1}^{(r)}(p)| \ = \ \varphi(p^k) - p^{k-1} \ = \ p^k - 2p^{k-1}. \end{aligned}$$

It follows that for any $s \in \mathbb{N}$ we have

$$\begin{aligned} \sum_{a \in \mathbb{Z}_{p^k}^*} \gcd(p^k, a-r)^s &= \sum_{j=0}^{k-1} |N_{k,j}^{(r)}(p)| p^{sj} + |M_{k,k}^{(r)}(p)| p^{sk} \\ &= p^k - 2p^{k-1} + p^k \sum_{j=1}^{k-1} (p^{(s-1)j} - p^{(s-1)j-1}) + p^{sk} \end{aligned} \tag{17}$$

which for $s=1$ turns into

$$\sum_{a \in \mathbb{Z}_{p^k}^*} \gcd(p^k, a-r) \ = \ (k+1)\varphi(p^k). \tag{18}$$

Now we compute $g_i(p^k)$ for $i = 1, 2, 3, 4$.

(i) By (17) with $r=1$ and $s=2$ we have

$$g_1(p^k)\varphi(p^k) \ = \ \sum_{a \in \mathbb{Z}_{p^k}^*} \gcd(p^k, a-1)^2 \ = \ p^{k-1}((p+1)p^k - 2),$$

and so $g_1(p^k) = ((p+1)p^k - 2)/(p-1)$ as claimed in (3).

(ii) For $p = 2$ and $k \geq 2$ we find, using (18) in the next-to-last step, that

$$\begin{aligned}
g_2(2^k)\varphi(2^k) &= \sum_{a \in \mathbb{Z}^*_{2^k}} \gcd(2^k, a-1)\gcd(2^k, a+1) \\
&= \sum_{j=0}^{2^{k-1}-1} \gcd(2^k, 2j)\gcd(2^k, 2j+2) \\
&= 4\sum_{j=0}^{2^{k-1}-1} \gcd(2^{k-1}, j)\gcd(2^{k-1}, j+1) \qquad (19) \\
&= 4\sum_{i=0}^{2^{k-2}-1} \gcd(2^{k-1}, 2i)\gcd(2^{k-1}, 2i+1) \\
&\qquad + 4\sum_{i=0}^{2^{k-2}-1} \gcd(2^{k-1}, 2i+1)\gcd(2^{k-1}, 2i+2) \\
&= 4\sum_{i=0}^{2^{k-2}-1} \gcd(2^{k-1}, 2i) + 4\sum_{i=0}^{2^{k-2}-1} \gcd(2^{k-1}, 2i+2) \\
&= 8\sum_{i=0}^{2^{k-2}-1} \gcd(2^{k-1}, 2i) = 8\sum_{a \in \mathbb{Z}^*_{2^{k-1}}} \gcd(2^{k-1}, a-1) \\
&= 8k\,\varphi(2^{k-1}) = 4k\,\varphi(2^k), \qquad (20)
\end{aligned}$$

as claimed in (4). The case $k = 1$ is easily verified directly.

If $p > 2$ then at most one of $a-1$, $a+1$ is divisible by p. Hence we find, using (18), that

$$\begin{aligned}
g_2(p^k)\varphi(p^k) &= \sum_{a \in \mathbb{Z}^*_{p^k}} \gcd(p^k, a-1)\gcd(p^k, a+1) \\
&= \sum_{a \in \mathbb{Z}^*_{p^k}} \gcd(p^k, a-1) + \sum_{a \in \mathbb{Z}^*_{p^k}} \gcd(p^k, a+1) - \sum_{a \in \mathbb{Z}^*_{p^k}} 1 \\
&= 2(k+1)\,\varphi(p^k) - \varphi(p^k) = (2k+1)\,\varphi(p^k)
\end{aligned}$$

and (4) follows.

(iii) For $p = 2$ and $k \geq 2$ we obtain

$$\begin{aligned}
g_3(2^k)\varphi(2^k) &= \sum_{a\in\mathbb{Z}^*_{2^k}} \gcd(2^k, a^2-1) \;=\; \sum_{j=0}^{2^{k-1}-1} \gcd(2^k, (2j+1)^2-1) \\
&= 4\sum_{j=0}^{2^{k-1}-1} \gcd(2^{k-2}, j(j+1)) \\
&= 4\sum_{j=0}^{2^{k-1}-1} \gcd(2^{k-2}, j)\gcd(2^{k-2}, j+1) \\
&= 4\sum_{j=0}^{2^{k-2}-1} \gcd(2^{k-2}, j)\gcd(2^{k-2}, j+1) \\
&+ 4\sum_{j=0}^{2^{k-2}-1} \gcd(2^{k-2}, j+2^{k-2})\gcd(2^{k-2}, j+1+2^{k-2}) \\
&= 8\sum_{j=0}^{2^{k-2}-1} \gcd(2^{k-2}, j)\gcd(2^{k-2}, j+1) \\
&= 8(k-1)\varphi(2^{k-1}) \;=\; 4(k-1)\varphi(2^k)
\end{aligned}$$

by (19) and (20). The case $k = 1$ is easily verified directly.

If $p > 2$ then at most one of $a-1$, $a+1$ is divisible by p. It follows that $\gcd(p^k, a^2-1) = \gcd(p^k, a-1)\gcd(p^k, a+1)$, and so $g_3(p^k) = g_2(p^k) = 2k+1$, proving (5).

(iv) For $p = 2$ we have

$$\begin{aligned}
g_4(2^k)\varphi(2^k) &= \sum_{a\in\mathbb{Z}^*_{2^k}} \gcd(2^k, a^2+1) \;=\; \sum_{j=0}^{2^{k-1}-1} \gcd(2^k, (2j+1)^2+1) \\
&= 2\sum_{j=0}^{2^{k-1}-1} \gcd(2^{k-1}, 2j^2+2j+1) \;=\; 2\cdot 2^{k-1} \;=\; 2\,\varphi(2^k).
\end{aligned}$$

Assume that $p \equiv 1 \pmod 4$. Then -1 is a quadratic residue modulo p^k, so there is an $r \in \mathbb{Z}$ such that $r^2 \equiv -1 \pmod{p^k}$. By Lemma 3.5 (i), $\gcd(p^k, a^2+1) = \gcd(p^k, a^2-r^2)$, hence

$$\begin{aligned}
g_4(p^k)\varphi(p^k) &= \sum_{a\in\mathbb{Z}^*_{p^k}} \gcd(p^k, a^2+1) \;=\; \sum_{a\in\mathbb{Z}^*_{p^k}} \gcd(p^k, a^2-r^2) \\
&= \sum_{a\in\mathbb{Z}^*_{p^k}} \gcd(p^k, (a-r)(a+r)).
\end{aligned}$$

If $p \mid a-r$ and $p \mid a+r$ then $p \mid 2a$ which is false, since p is odd and $a \in \mathbb{Z}_{p^k}^*$. Hence at most one of $a-r$, $a+r$ is divisible by p. Now by the same argument as in (ii) we find that $g_4(p^k)\varphi(p^k) = (2k+1)\varphi(p^k)$, hence $g_4(p^k) = 2k+1$.

Finally, let $p \equiv 3 \pmod 4$. Then -1 is a quadratic nonresidue modulo p, hence $\gcd(p^k, a^2+1) = 1$ for all a. It follows that

$$g_4(p^k)\varphi(p^k) \;=\; \sum_{a \in \mathbb{Z}_{p^k}^*} \gcd(p^k, a^2+1) \;=\; \varphi(p^k)$$

and so $g_4(p^k) = 1$, proving (6). □

It remains to show that $g_1(n)$, $g_2(n)$, $g_3(n)$, $g_4(n)$ are multiplicative.

Lemma 3.12 *Let*

$$g(n) \;=\; \sum_{a \in \mathbb{Z}_n^*} \prod_{k=1}^{r} \gcd(n, P_k(a))$$

where $P_1(x), P_2(x), \ldots, P_r(x)$ are polynomials in x with integer coefficients. Then $g(n)$ is a multiplicative arithmetic function.

Proof: Let $n = n_1 n_2$ where $\gcd(n_1, n_2) = 1$. We need to show that $g(n) = g(n_1)g(n_2)$. For $a \in \mathbb{Z}_n$, let $a_1 \in \mathbb{Z}_{n_1}$ and $a_2 \in \mathbb{Z}_{n_2}$ be such that

$$a \equiv a_1 \pmod{n_1}, \quad a \equiv a_2 \pmod{n_2}.$$

By the Chinese Remainder Theorem, the mapping

$$f: \; a \mapsto (a_1, a_2)$$

is a bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. By Lemma 3.5 (i) and (ii), $\gcd(n_1 n_2, a) = 1$ iff $\gcd(n_1, a) = \gcd(n_2, a) = 1$ iff $\gcd(n_1, a_1) = \gcd(n_2, a_2) = 1$, therefore f restricted to $\mathbb{Z}_n^*$ is a bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$. Also, $P_k(a) \equiv P_k(a_i) \pmod{n_i}$ for $i = 1, 2$, hence by Lemma 3.5 (i) and (ii),

$$\begin{aligned} \gcd(n_1 n_2, P_k(a)) &= \gcd(n_1, P_k(a)) \gcd(n_2, P_k(a)) \\ &= \gcd(n_1, P_k(a_1)) \gcd(n_2, P_k(a_2)). \end{aligned}$$

It follows that

$$\begin{aligned} g(n_1 n_2) &= \sum_{(a_1, a_2) \in \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*} \prod_{k=1}^{r} \gcd(n_1, P_k(a_1)) \gcd(n_2, P_k(a_2)) \\ &= \sum_{a_1 \in \mathbb{Z}_{n_1}} \prod_{k=1}^{r} \gcd(n_1, P_k(a_1)) \sum_{a_2 \in \mathbb{Z}_{n_2}} \prod_{k=1}^{r} \gcd(n_2, P_k(a_2)) \\ &= g(n_1) g(n_2), \end{aligned}$$

proving multiplicativity of $g(n)$. $\square$

Proof of Theorem 2.1:

Clearly $I(n) = |\mathcal{K}_n/\simeq|$, and the assumptions of Lemma 3.9 are satisfied. We still need to compute $\nu_0(\mathbb{Z}_n \times \mathbb{Z}_n)$. From Corollary 3.4 (iii) it follows that the set $U_n := (\{0\} \times \mathbb{Z}_n) \cup (\mathbb{Z}_n \times \{0\})$ equals the union of $\tau(n)$ orbits with representatives $(0, k)$ where $k \mid n$ (with $k = n$ replaced by 0). So if n is odd, $\nu_0(\mathbb{Z}_n \times \mathbb{Z}_n) = \tau(n)$. If n is even, the set $V_n := (\{n/2\} \times \mathbb{Z}_n) \cup (\mathbb{Z}_n \times \{n/2\})$ equals the union of $\tau(n)$ orbits with representatives $(n/2, k)$ where $k \mid n$ (with n replaced by 0). The two sets U_n and V_n share the orbit containing $(n/2, 0)$, hence in this case $\nu_0(\mathbb{Z}_n \times \mathbb{Z}_n)$ $= 2\tau(n) - 1$. Equation (2) now follows by Lemma 3.9, using Proposition 3.10, Lemma 3.11 and Lemma 3.12. $\square$

3.3 Generalized Petersen graphs

Let $\mathcal{K}_n$ be the set of all generalized Petersen graphs on $2n$ vertices, and

$$K_n := \mathbb{Z}_n^* \times \mathbb{Z}_n \ \cup \ \mathbb{Z}_n \times \mathbb{Z}_n^*.$$

Proposition 3.13

$$|K_n/\sim_{\alpha_n}| \ = \ \frac{1}{4}(2n - \varphi(n) + 2\gcd(n, 2) + r(n) + s(n)) \qquad (21)$$

Proof: We use Lemma 3.1. Assume that $(j, k) \in K_n$ is fixed by some $g \in G_n$.

a) If $g = \xi_a$ then $(aj, ak) = (j, k)$. Since $\{j, k\} \cap \mathbb{Z}_n^* \neq \emptyset$, it follows that $a \equiv 1 \pmod{n}$. So $\sum_{a \in \mathbb{Z}_n^*} \mathrm{fix}_{\alpha_n}(\xi_a) = \mathrm{fix}_{\alpha_n}(\xi_1) = |K_n| = n^2 - (n - \varphi(n))^2 = \varphi(n)(2n - \varphi(n))$.

b) If $g = \xi_a \mu$ then $(aj, -ak) = (j, k)$. Since $\{j, k\} \cap \mathbb{Z}_n^* \neq \emptyset$, it follows that $a \equiv \pm 1 \pmod{n}$. In one case, $2k \equiv 0 \pmod{n}$, so $k = 0$ or $k = n/2$ if n is even, and $j \in \mathbb{Z}_n^*$. In the other, the roles of j and k are reversed. So $\mathrm{fix}_{\alpha_n}(\xi_1 \mu) = \mathrm{fix}_{\alpha_n}(\xi_{-1} \mu) = \gcd(n, 2)\varphi(n)$, and $\sum_{a \in \mathbb{Z}_n^*} \mathrm{fix}_{\alpha_n}(\xi_a \mu) = 2\gcd(n, 2)\varphi(n)$.

c) If $g = \xi_a \rho$ then $(ak, aj) = (j, k)$. In this case $a^2 j \equiv j \pmod{n}$ and $a^2 k \equiv k \pmod{n}$, so $a^2 \equiv 1 \pmod{n}$, $j, k \in \mathbb{Z}_n^*$, and $k \equiv aj \pmod{n}$ is determined by the choice of $j \in \mathbb{Z}_n^*$. Thus $\sum_{a \in \mathbb{Z}_n^*} \mathrm{fix}_{\alpha_n}(\xi_a \rho) = r(n)\varphi(n)$.

d) If $g = \xi_a \rho \mu$ then $(-ak, aj) = (j, k)$. In this case $a^2 j \equiv -j \pmod{n}$ and $a^2 k \equiv -k \pmod{n}$, so $a^2 \equiv -1 \pmod{n}$, $j, k \in \mathbb{Z}_n^*$, and $k \equiv aj \pmod{n}$ is determined by the choice of $j \in \mathbb{Z}_n^*$. Thus $\sum_{a \in \mathbb{Z}_n^*} \mathrm{fix}_{\alpha_n}(\xi_a \rho \mu) = s(n)\varphi(n)$.

Equation (21) now follows from Lemma 3.1. $\square$

Proof of Theorem 2.2:

Clearly $P(n) = |\mathcal{K}_n/\simeq|$. It follows from Theorem 1.1 that $I(n, j, k)$ is isomorphic to a generalized Petersen graph if and only if $j \in \mathbb{Z}_n^*$ or $k \in \mathbb{Z}_n^*$, hence the assumptions of Lemma 3.9 are satisfied. We still need to compute $\nu_0(K_n)$, the number of orbits containing pairs of the form $(0, k)$ or $(n/2, k)$ with $k \in \mathbb{Z}_n^*$. There are two such orbits if n is even, and one if n is odd, hence $\nu_0(K_n) = \gcd(n, 2)$. Equation (7) now follows by Lemma 3.9, using Proposition 3.13. □

3.4 Connected I-graphs

Let $\mathcal{K}_n$ be the set of all connected I-graphs on $2n$ vertices, and

$$K_n \;:=\; \{(j,k) \in \mathbb{Z}_n \times \mathbb{Z}_n;\ \gcd(n,j,k) = 1\}.$$

Proposition 3.14

$$|K_n/{\sim_{\alpha_n}}| \;=\; \frac{1}{4}\left(\frac{J_2(n)}{\varphi(n)} + r(n) + s(n) + t(n)\right) \tag{22}$$

where $t(n) = t_1(n) + t_2(n)$ is given in (9).

Proof: We use Lemma 3.1. Assume that $(j, k) \in K_n$ is fixed by some $g \in G_n$.

a) If $g = \xi_a$ then $(aj, ak) = (j, k)$. Let $d = \gcd(n, a-1)$, $n = n'd$ and $a - 1 = a'd$. As in the proof of Proposition 3.2, we see that $n' \,|\, j$ and $n' \,|\, k$. Since $n' \,|\, n$ as well, it follows that $n' = 1$ and so $n \,|\, a-1$, which is only possible if $a = 1$. Thus ξ_a has no fixed points unless $a = 1$. As ξ_1 fixes all points in K_n, we have

$$\sum_{a \in \mathbb{Z}_n^*} \mathrm{fix}_{\alpha_n}(\xi_a) \;=\; \mathrm{fix}_{\alpha_n}(\xi_1) \;=\; |K_n| \;=\; J_2(n).$$

b) If $g = \xi_a\mu$ then $(aj, -ak) = (j, k)$. Denote $n_j = \gcd(n, j)$ and $n_k = \gcd(n, k)$. Any common divisor of n_j and n_k is a common divisor of n, j, k, hence $n_j \perp n_k$ and $n_j n_k \,|\, n$. Denote $n_0 = n/(n_j n_k)$, $j' = j/n_j$, $k' = k/n_k$. Then

$$n \;=\; n_0 n_j n_k,\ j' \in \mathbb{Z}_{n_0 n_k}^*,\ k' \in \mathbb{Z}_{n_0 n_j}^*.$$

From $aj \equiv j \pmod n$ it follows that $n_0 n_k \,|\, (a-1)j'$, hence $n_0 n_k \,|\, a-1$. From $ak \equiv -k \pmod n$ it follows that $n_0 n_j \,|\, (a+1)k'$, hence $n_0 n_j \,|\, a+1$. Therefore $n_0 \,|\, 2$, and so $n_0 \in \{1, 2\}$ and $\varphi(n_0) = 1$.

We claim that for each pair (j, k) where $j = j'n_j$, $k = k'n_k$, $n = n_0 n_j n_k$, $n_0 \in \{1, 2\}$, $n_j \perp n_k$, $j' \in \mathbb{Z}_{n_0 n_k}^*$ and $k' \in \mathbb{Z}_{n_0 n_j}^*$, there is a unique $a \in \mathbb{Z}_n^*$ such that $aj \equiv j \pmod n$ and $ak \equiv -k \pmod n$. Indeed, let $n = \prod_{i=1}^m p_i^{e_i}$ be the prime factorization of n (i.e., $p_1, p_2, \ldots, p_m$ are distinct primes and $e_i \geq 1$ for $i = 1, 2, \ldots, m$). Define $a \in \mathbb{Z}$ by requiring that for each $i \in \{1, 2, \ldots, m\}$,

$$\begin{aligned} a &\equiv -1 \pmod{p_i^{e_i}} \quad \text{if } p_i^{e_i} \,|\, n_0 n_j, \\ a &\equiv 1 \pmod{p_i^{e_i}} \quad \text{if } p_i^{e_i} \,|\, n_0 n_k. \end{aligned}$$

At least one of $p_i^{e_i} \,|\, n_0 n_j$ and $p_i^{e_i} \,|\, n_0 n_k$ holds for each $i \in \{1, 2, \ldots, m\}$, and both hold only if $p_i^{e_i} = n_0 = 2$, hence these requirements are consistent, and by the Chinese Remainder Theorem, there is a unique $a \in \mathbb{Z}_n$ which satisfies them. In fact, $a^2 \equiv 1 \pmod{p_i^{e_i}}$ for $i = 1, 2, \ldots, m$, hence $a^2 \equiv 1 \pmod{n}$, and so $a \in \mathbb{Z}_n^*$. Note that a is odd if $n_0 = 2$, therefore $n_0 \,|\, a - 1$ and $n_0 \,|\, a + 1$.

If $p_i^{e_i} \,|\, n_0 n_j$ then $p_i^{e_i} \,|\, n_0 j \,|\, (a-1)j$. Also, $a \equiv -1 \pmod{p_i^{e_i}}$, so $p_i^{e_i} \,|\, (a+1)k$.

If $p_i^{e_i} \,|\, n_0 n_k$ then $p_i^{e_i} \,|\, n_0 k \,|\, (a+1)k$. Also, $a \equiv 1 \pmod{p_i^{e_i}}$, so $p_i^{e_i} \,|\, (a-1)j$.

In either case, $p_i^{e_i} \,|\, (a-1)j$ and $p_i^{e_i} \,|\, (a+1)k$. As this holds for all $i \in \{1, 2, \ldots, m\}$, it follows that $n \,|\, (a-1)j$ and $n \,|\, (a+1)k$, hence $aj \equiv j \pmod{n}$ and $ak \equiv -k \pmod{n}$ as claimed.

Thus to construct $(j, k) \in K_n$ which is fixed by some $\xi_a \mu$, first select n_0, n_j, n_k, j', $k' \in \mathbb{Z}_n$ such that $n_0 \in \{1, 2\}$, $n_j \perp n_k$, $n = n_0 n_j n_k$, $j' \in \mathbb{Z}_{n_0 n_k}^*$ and $k' \in \mathbb{Z}_{n_0 n_j}^*$, then take $j = j' n_j$, $k = k' n_k$. This can be done in

$$\sum_{n_0 \in \{1,2\}, n_j \perp n_k, n = n_0 n_j n_k} \varphi(n_0 n_k) \varphi(n_0 n_j)$$

ways. W.l.g. assume that n_k is odd. Then $\varphi(n_0 n_k)\varphi(n_0 n_j) = \varphi(n_0)\varphi(n_k)\varphi(n_0 n_j)$ $= \varphi(n_k)\varphi(n_0 n_j) = \varphi(n_0 n_j n_k) = \varphi(n)$, hence

$$\sum_{a \in \mathbb{Z}_n^*} \text{fix}_{\alpha_n}(\xi_a \mu) \;=\; \varphi(n)(t_1(n) + t_2(n))$$

where $t_{n_0}(n) \;=\; |\{(n_j, n_k);\; n_j \perp n_k, n = n_0 n_j n_k\}|$. Clearly, $t_1(n) = 2^{\omega(n)}$ and

$$t_2(n) \;=\; \begin{cases} 2^{\omega(n/2)}, & n \text{ even}, \\ 0, & n \text{ odd}. \end{cases}$$

c) If $g = \xi_a \rho$ then $(ak, aj) = (j, k)$. In this case $\gcd(n, j, aj) = \gcd(n, j, k) = 1$ by Lemma 3.5 (i), and $a^2 j \equiv j \pmod{n}$. It follows that $j \in \mathbb{Z}_n^*$ and $a^2 \equiv 1 \pmod{n}$. Since $k \equiv aj \pmod{n}$ is determined by the choice of $j \in \mathbb{Z}_n^*$, we have $\sum_{a \in \mathbb{Z}_n^*} \text{fix}_{\alpha_n}(\xi_a \rho) = r(n)\varphi(n)$.

d) If $g = \xi_a \rho \mu$ then $(-ak, aj) = (j, k)$. In this case $\gcd(n, j, aj) = \gcd(n, j, k)$ $= 1$ by Lemma 3.5 (i), and $a^2 j \equiv -j \pmod{n}$. It follows that $j \in \mathbb{Z}_n^*$ and $a^2 \equiv -1 \pmod{n}$. Since $k \equiv aj \pmod{n}$ is determined by the choice of $j \in \mathbb{Z}_n^*$, we have $\sum_{a \in \mathbb{Z}_n^*} \text{fix}_{\alpha_n}(\xi_a \rho \mu) = s(n)\varphi(n)$.

Equation (22) now follows from Lemma 3.1. □

Proof of Theorem 2.3:

Clearly $I_c(n) = |\mathcal{K}_n/\simeq|$. It follows from Theorem 1.2 that the assumptions of Lemma 3.9 are satisfied. We still need to compute $\nu_0(K_n)$, the number of orbits containing pairs of the form $(0,k)$ or $(n/2,k)$ with $k \in \mathbb{Z}_n^*$.

If $(0,k) \in K_n$ then $\gcd(n,k) = \gcd(n,0,k) = 1$, hence $k \in \mathbb{Z}_n^*$. It follows that all such pairs belong to a single orbit of α_n.

Assume that $n \equiv 0 \pmod 4$. If $(n/2,k) \in K_n$ then $\gcd(n, n/2, k) = 1$. Since in this case $\gcd(n,n/2,k) = 1$ iff $\gcd(n,k) = 1$, it follows that $k \in \mathbb{Z}_n^*$. For any $a \in \mathbb{Z}_n^*$ we have $a(n/2) \equiv n/2 \pmod n$, hence we conclude again that all such pairs belong to a single orbit of α_n.

Assume that $n \equiv 2 \pmod 4$. If $(n/2,k) \in K_n$ then $\gcd(n,n/2,k) = 1$. In this case it is straightforward to see that $\gcd(n,n/2,k) = 1$ iff $k = 2^j a$ for some $j \geq 0$ and $a \in \mathbb{Z}_n^*$. All the pairs $(n/2,a)$ with $a \in \mathbb{Z}_n^*$ clearly belong to a single orbit of α_n. Now we claim that $4\mathbb{Z}_n^* = 2\mathbb{Z}_n^*$. Indeed, let $q = n/2$ and $a \in \mathbb{Z}_n^*$. Then $\gcd(2a+q,n) = 1$ and $4a \equiv 2(2a+q) \pmod n$, proving that $4\mathbb{Z}_n^* \subseteq 2\mathbb{Z}_n^*$. Conversely, if $q \equiv 1 \pmod 4$ then $\gcd((q+1)/2, n) = 1$ and $2a \equiv 4a(q+1)/2 \pmod n$. If $q \equiv 3 \pmod 4$ then $\gcd((3q+1)/2, n) = 1$ and $2a \equiv 4a((3q+1)/2) \pmod n$, proving that $2\mathbb{Z}_n^* \subseteq 4\mathbb{Z}_n^*$, and also the claim. Hence all the pairs $(n/2, 2^j a)$ with $j \geq 1$ and $a \in \mathbb{Z}_n^*$ also belong to a single orbit of α_n. On the other hand, all the pairs in the orbit of $(n/2,1)$ have one component in $\mathbb{Z}_n^*$, while all the pairs in the orbit of $(n/2,2)$ have neither component in $\mathbb{Z}_n^*$, hence these two orbits are distinct.

It follows that

$$\nu_0(K_n) = \begin{cases} 1, & n \equiv 1 \pmod 2, \\ 2, & n \equiv 0 \pmod 4, \\ 3, & n \equiv 2 \pmod 4, \end{cases}$$

which together with Lemma 3.9 and Proposition 3.14 yields (8). □

3.5 Bipartite generalized Petersen graphs

Let $\mathcal{K}_n$ be the set of all bipartite generalized Petersen graphs on $2n$ vertices, and

$$K_n := \mathbb{Z}_n^* \times \mathbb{Z}_n^o \ \cup \ \mathbb{Z}_n^o \times \mathbb{Z}_n^*,$$

where $\mathbb{Z}_n^o$ is the subset of odd elements in $\mathbb{Z}_n$.

Proposition 3.15 *Let n be even. Then*

$$|K_n/\sim_{\alpha_n}| = \frac{1}{4}\left(n - \varphi(n) + 2\left((n/2) \bmod 2\right) + r(n) + s(n)\right). \tag{23}$$

Proof: We follow the proof of Proposition 3.13. Assume that $(j,k) \in K_n$ is fixed by some $g \in G_n$, and notice that both j and k are odd.

a) If $g = \xi_a$ then $(aj, ak) = (j, k)$. From $\{j,k\} \cap \mathbb{Z}_n^* \neq \emptyset$ it follows that $a \equiv 1 \pmod{n}$. So $\sum_{a \in \mathbb{Z}_n^*} \mathrm{fix}_{\alpha_n}(\xi_a) = |K_n| = (n/2)^2 - (n/2 - \varphi(n))^2 = \varphi(n)(n - \varphi(n))$.

b) If $g = \xi_a \mu$ then $(aj, -ak) = (j, k)$. If $j \in \mathbb{Z}_n^*$, then $a \equiv 1 \pmod{n}$ and $2k \equiv 0 \pmod{n}$. As k is odd, this is only possible if $n \not\equiv 0 \pmod{4}$ and $k = n/2$. If $k \in \mathbb{Z}_n^*$, then $a \equiv -1 \pmod{n}$, $n \not\equiv 0 \pmod{4}$ and $j = n/2$. So $\mathrm{fix}_{\alpha_n}(\xi_1 \mu) = \mathrm{fix}_{\alpha_n}(\xi_{-1}\mu) = \varphi(n)(n/2 \pmod{2})$, and $\sum_{a \in \mathbb{Z}_n^*} \mathrm{fix}_{\alpha_n}(\xi_a \mu) = 2\varphi(n)(n/2 \pmod{2})$.

c), d): As in the proof of Proposition 3.13.

Equation (23) now follows from Lemma 3.1. □

Proof of Theorem 2.4:

Clearly $P_b(n) = |\mathcal{K}_n/\simeq|$. It follows from Theorems 1.1 and 1.3 that $I(n,j,k)$ is isomorphic to a bipartite generalized Petersen graph if and only if $j \in \mathbb{Z}_n^*$ and k is odd, or $k \in \mathbb{Z}_n^*$ and j is odd, hence the assumptions of Lemma 3.9 are satisfied. We still need to compute $\nu_0(K_n)$, the number of orbits containing pairs of the form $(n/2, k)$ with $n/2$ odd and $k \in \mathbb{Z}_n^*$. There are no such orbits if $n \equiv 0 \pmod{4}$, and one such orbit if $n \equiv 2 \pmod{4}$. Hence

$$\nu_0(K_n) = (n/2) \bmod 2,$$

which together with Lemma 3.9 and Proposition 3.15 yields (10). □

3.6 Bipartite connected I-graphs

Let $\mathcal{K}_n$ be the set of all bipartite connected I-graphs on $2n$ vertices, and

$$K_n := \{(j,k) \in \mathbb{Z}_n \times \mathbb{Z}_n;\ \gcd(n,j,k) = 1,\ j,k \text{ odd}\}.$$

Proposition 3.16 *Let n be even. Then*

$$|K_n/{\sim_{\alpha_n}}| = \frac{1}{4}\left(\frac{J_2(n)}{3\varphi(n)} + ((n/2) \bmod 2)\, 2^{\omega(n/2)} + r(n) + s(n)\right). \qquad (24)$$

Proof: We follow the proof of Proposition 3.14. Assume that $(j,k) \in K_n$ is fixed by some $g \in G_n$.

a) If $g = \xi_a$ then $(aj, ak) = (j,k)$. As in case a) in the proof of Proposition 3.14, we see that $a \equiv 1 \pmod{n}$, thus $\sum_{a \in \mathbb{Z}_n^*} \mathrm{fix}_{\alpha_n}(\xi_a) = \mathrm{fix}_{\alpha_n}(\xi_1) = |K_n|$. Let

$$\begin{aligned} U_n &:= \{(j,k) \in \mathbb{Z}_n \times \mathbb{Z}_n;\ \gcd(n,j,k) = 1,\ j \text{ odd}, k \text{ even}\}, \\ V_n &:= \{(j,k) \in \mathbb{Z}_n \times \mathbb{Z}_n;\ \gcd(n,j,k) = 1,\ j \text{ even}, k \text{ odd}\}, \\ W_n &:= \{(j,k) \in \mathbb{Z}_n \times \mathbb{Z}_n;\ \gcd(n,j,k) = 1\}. \end{aligned}$$

Define the functions $f_n : K_n \to U_n$ and $g_n : U_n \to K_n$ by

$$\begin{aligned} f_n(j,k) &:= (j, k+j) \pmod{n}, \\ g_n(j,k) &:= (j, k-j) \pmod{n}. \end{aligned}$$

Clearly $\gcd(n,j,k) = 1$ iff $\gcd(n,j,k+j) = 1$ iff $\gcd(n,j,k-j) = 1$. Next, for j,k odd, $k+j \pmod{n}$ is even, and if j is odd and k is even, then $k-j \pmod{n}$ is odd. Since $f_n(g_n(j,k)) = (j,k) = g_n(f_n(j,k))$, we conclude that f_n and g_n are bijections, and $|K_n| = |U_n|$. Since $W_n = K_n \cup U_n \cup V_n$, $|W_n| = J_2(n)$, and $|U_n| = |V_n|$ by symmetry, it follows that $|K_n| = |U_n| = |V_n| = J_2(n)/3$.

b) If $g = \xi_a\mu$ then $(aj, -ak) = (j,k)$. As in case b) in the proof of Proposition 3.14, we see that $n = n_0 n_j n_k$ where $n_0 \,|\, 2$, $n_j \,|\, j$ and $n_k \,|\, k$. Since n is even while j and k are odd, it follows that $n_0 = 2$, hence $\xi_a\mu$ has no fixed points if $n \equiv 0 \pmod 4$. So assume that $n \equiv 2 \pmod 4$. To construct $(j,k) \in K_n$ which is fixed by some (uniquely determined) $\xi_a\mu$, first select $n_j, n_k, j', k' \in \mathbb{Z}_n$ such that $n_j \perp n_k$, $n = 2n_j n_k$, $j' \in \mathbb{Z}^*_{2n_k}$ and $k' \in \mathbb{Z}^*_{2n_j}$, then take $j = j'n_j$, $k = k'n_k$. This can be done in

$$\sum_{n_j \perp n_k, n = 2n_j n_k} \varphi(2n_k)\varphi(2n_j)$$

ways. Since n_k and n_j are odd, $\varphi(2n_k)\varphi(2n_j) = \varphi(n_k)\varphi(2n_j) = \varphi(2n_k n_j) = \varphi(n)$. Therefore $\sum_{a \in \mathbb{Z}^*_n} \mathrm{fix}_{\alpha_n}(\xi_a\mu) = \varphi(n)\, 2^{\omega(n/2)}$ if $n \equiv 2 \pmod 4$. By multiplying this expression with $(n/2) \bmod 2$ we extend its validity to all even n.

c), d): As in the proof of Proposition 3.14.

Equation (24) now follows from Lemma 3.1. □

Proof of Theorem 2.5:

Clearly $I_{bc}(n) = |\mathcal{K}_n/\simeq|$. It follows from Theorems 1.2 and 1.3 that the assumptions of Lemma 3.9 are satisfied. We still need to compute $\nu_0(K_n)$, the number of orbits containing pairs of the form $(n/2, k)$ with $n/2$ and k odd and $\gcd(n, n/2, k) = 1$. In this case $\gcd(n, n/2, k) = 1$ if and only if $\gcd(n,k) = 1$. Therefore there are no such orbits if $n \equiv 0 \pmod 4$, and one such orbit if $n \equiv 2 \pmod 4$. Hence

$$\nu_0(K_n) = (n/2) \bmod 2,$$

which together with Lemma 3.9 and Proposition 3.16 yields (11). □

4 Concluding remark

It is not difficult to see that the numbers $I_c(n)$ and $I(n)$ of isomorphism classes of connected I-graphs resp. all I-graphs on $2n$ vertices satisfy the pair of Moebius inverse relations

$$I(n) \;=\; \sum_{d\,|\,n} I_c(d), \quad I_c(n) \;=\; \sum_{d\,|\,n} \mu(n/d) I(d)$$

(cf. [8, Sec. 3]).

References

[1] M. Boben, T. Pisanski, A. Žitnik, I-graphs and the corresponding configurations, *J. Combin. Des.* **13** (2005) 406–424.

[2] I. Z. Bouwer, W. W. Chernoff, B. Monson, Z. Star, *The Foster Census*, Charles Babbage Research Centre, 1988.

[3] R. Frucht, J. E. Graver, M. E. Watkins, The groups of the generalized Petersen graphs, *Proc. Camb. Phil. Soc.* **70** (1971) 211–218.

[4] B. Horvat, T. Pisanski, A. Žitnik, All generalized Petersen graphs are unit-distance graphs, submitted.

[5] B. Horvat, T. Pisanski, A. Žitnik, Isomorphism checking of I-graphs, submitted.

[6] V. A. Liskovets, A. D. Mednykh, On the number of connected and disconnected coverings over a manifold, *Ars Math. Contemp.* **2** (2009) 181–189.

[7] A. Orbanić, M. Petkovšek, T. Pisanski, P. Potočnik, A note on enumeration of one-vertex maps, *Ars Math. Contemp.*, to appear.

[8] M. Petkovšek, T. Pisanski, Counting disconnected structures: chemical trees, fullerenes, I-graphs, and others, *Croat. Chem. Acta* **78** (2005) 563–567.

[9] T. Pisanski, D. Schattschneider, B. Servatius, Applying Burnside's lemma to a one-dimensional Escher problem, *Math. Mag.* **79** (2006) 167–180.

[10] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at `http://www.research.att.com/ njas/sequences/`.

[11] R. P. Stanley, *Enumerative Combinatorics*, vol. 2, Cambridge University Press, Cambridge 1999.

[12] A. Steimle, W. Staton, The isomorphism classes of the generalized Petersen graphs, *Discrete Math.* **309** (2009) 231–237.

[13] M. E. Watkins, A theorem on Tait colorings with an application to the generalized Petersen graphs, *J. Comb. Theory* **6** (1969) 152–164.