# On restricted unitary Cayley graphs and symplectic transformations modulo $n$

Niel de Beaudrap*

Quantum Information Theory Group
Institut für Physik und Astronomie, Universität Potsdam

Submitted: Feb 12, 2010; Accepted: Apr 27, 2010; Published: May 7, 2010
Mathematics Subject Classification: 05C12, 05C17, 05C50

**Abstract**

We present some observations on a restricted variant of unitary Cayley graphs modulo $n$, and implications for a decomposition of elements of symplectic operators over the integers modulo $n$. We define *quadratic unitary Cayley graphs* $G_n$, whose vertex set is the ring $\mathbb{Z}_n$, and where residues $a, b$ modulo $n$ are adjacent if and only if their difference is a quadratic residue. By bounding the diameter of such graphs, we show an upper bound on the number of elementary operations (symplectic scalar multiplications, symplectic row swaps, and row additions or subtractions) required to decompose a symplectic matrix over $\mathbb{Z}_n$. We also characterize the conditions on $n$ for $G_n$ to be a perfect graph.

## 1 Introduction

For an integer $n \geqslant 1$, we denote the ring of integers modulo $n$ by $\mathbb{Z}_n$, and the group of multiplicative units modulo $n$ by $\mathbb{Z}_n^\times$. A well-studied family of graphs are the *unitary Cayley graphs* on $\mathbb{Z}_n$, which are defined by $X_n = \mathrm{Cay}(\mathbb{Z}_n, \mathbb{Z}_n^\times)$. These form the basis of the subject of graph representations [1], and are also studied as objects of independent interest: see for example [2–5].

We consider a subgraph $G_n \leqslant X_n$ of the unitary Cayley graphs, defined as follows. Let $Q_n = \left\{ u^2 \,\middle|\, u \in \mathbb{Z}_n^\times \right\}$ be the group of *quadratic units* modulo $n$ (quadratic residues which are also multiplicative units), and $T_n = \pm Q_n$. We then define $G_n = \mathrm{Cay}(\mathbb{Z}_n, T_n)$, in which two vertices given by $a, b \in \mathbb{Z}_n$ are adjacent if and only if their difference is a quadratic unit in $\mathbb{Z}_n$, *i.e.* if $a - b \in \left\{ \pm u^2 \,\middle|\, u \in \mathbb{Z}_n^\times \right\}$. In the case where $n \equiv 1 \pmod 4$ and is prime, $G_n$ coincides with the Paley graph on $n$ vertices: thus the graphs $G_n$ are a

*niel.debeaudrap@gmail.com

circulant generalization of these graphs for arbitrary $n$. We refer to $G_n$ as the *(undirected) quadratic unitary Cayley graph* on $\mathbb{Z}_n$.

We present some structural properties of quadratic unitary Cayley graphs $G_n$. In particular, we characterize its decompositions into tensor products over relatively prime factors of $n$, and categorize the graphs $G_n$ in terms of their diameters. From these results, we obtain a corollary regarding the decomposition of symplectic matrices $S \in \mathrm{Sp}_{2m}(\mathbb{Z}_n)$ in terms of symplectic row-operations, consisting of symplectic scalar multiplications, symplectic row-swaps, and symplectic row-additions/subtractions. We also characterize the conditions under which quadratic unitary graphs are perfect, by examining special cases of quadratic unitary graphs which are self-complementary.

**Notation.** Throughout the following, $n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ is a decomposition of $n$ into powers of distinct primes, and $\sigma : \mathbb{Z}_n \to \mathbb{Z}_{p_1{}^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t{}^{m_t}}$ is the isomorphism of rings which is induced by the Chinese Remainder theorem. (We refer to similar isomorphisms $\rho : \mathbb{Z}_n \longrightarrow \mathbb{Z}_M \oplus \mathbb{Z}_N$ for coprime $M$ and $N$ as *natural* isomorphisms.) We sometimes describe the properties of $G_n$ in terms of the directed Cayley graph $\Gamma_n = \mathrm{Cay}(\mathbb{Z}_n, Q_n)$, whose arcs $a \to b$ correspond to addition (but not subtraction) of a quadratic unit to a modulus $a \in \mathbb{Z}_n$; we may refer to this as the *directed quadratic unitary Cayley graph*.

# 2 Tensor product structure

By the isomorphism $\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1{}^{m_1}}^\times \oplus \cdots \oplus \mathbb{Z}_{p_t{}^{m_t}}^\times$ induced by $\sigma$, unitary Cayley graphs $X_n$ may be decomposed as *tensor products* $X_n \cong X_{p_1{}^{m_1}} \otimes \cdots \otimes X_{p_t{}^{m_t}}$ of smaller unitary Cayley graphs (also called direct products [5] or Kronecker products [6], among other terms):

**Definition I.** The *tensor product* $A \otimes B$ of two (di-)graphs $A$ and $B$ is the (di-)graph with vertex-set $V(A) \times V(B)$, where $((u,u'),(v,v')) \in E(A \otimes B)$ if and only if $((u,v),(u',v')) \in E(A) \times E(B)$.[1]

Corollary 3.3 of [5] gives an explicit proof that $X_n \cong X_{p_1{}^{m_1}} \otimes \cdots \otimes X_{p_t{}^{m_t}}$; a similar approach may be used to decompose any (di-)graph $\mathrm{Cay}(R, M)$ for rings $R = R_1 \oplus \cdots \oplus R_t$ and multiplicative monoids $M_1 = M_1 \oplus \cdots \oplus M_t$ where $M_j \subseteq R_j$. For instance, as $Q_n \cong Q_{p_1{}^{m_1}} \oplus \cdots \oplus Q_{p_t{}^{m_t}}$, it follows that $\Gamma_n \cong \Gamma_{p_1{}^{m_1}} \otimes \cdots \otimes \Gamma_{p_t{}^{m_t}}$ as well.

It is reasonable to suppose that the graphs $G_n$ will also exhibit tensor product structure; however, they do not always decompose over the prime power factors of $n$ as do $X_n$ and $\Gamma_n$. This is because $T_n$ may fail to decompose as a direct product of groups over the prime-power factors $p_j^{m_j}$. By definition, for each $j$, we either have $T_{p_j{}^{m_j}} = Q_{p_j{}^{m_j}}$ or $T_{p_j{}^{m_j}} \cong Q_{p_j{}^{m_j}} \oplus \langle -1 \rangle$; when $Q_{p_j{}^{m_j}} < T_{p_j{}^{m_j}}$ for multiple $p_j$, one cannot decompose $T_n$ over the prime-power factors of $n$. We may generalize this observation as follows:

**Theorem 1.** *For coprime integers $M, N \geqslant 1$, we have $G_M \otimes G_N \cong G_{MN}$ if and only if either $-1 \in Q_M$ or $-1 \in Q_N$.*

[1] We write $A_1 \otimes (A_2 \otimes A_3) = (A_1 \otimes A_2) \otimes A_3 = A_1 \otimes A_2 \otimes A_3$, and so on for higher-order tensor products, similarly to the convention for Cartesian products of sets.

*Proof.* We have $G_M \otimes G_N \cong G_{MN}$ if and only if $T_M \oplus T_N \cong T_{MN}$. Let $\rho : \mathbb{Z}_{MN} \longrightarrow \mathbb{Z}_M \oplus \mathbb{Z}_N$ be the natural isomorphism: this induces an isomorphism $Q_{MN} \cong Q_M \oplus Q_N$, and will also induce an isomorphism $T_{MN} \cong T_M \oplus T_N$ if the two groups are indeed isomorphic. Clearly, $\sigma(T_{MN}) \leqslant T_M \oplus T_N$; we consider the opposite inclusion.

If $-1 \notin Q_M$ and $-1 \notin Q_N$, we have $(-1,\, 1), (1, -1) \notin Q_M \oplus Q_N$; as both tuples are elements of $T_M \oplus T_N$, but neither of them are elements of $\pm(Q_M \oplus Q_N) = \sigma(\pm Q_{MN}) = \sigma(T_{MN})$, it follows that $T_{MN}$ and $T_M \oplus T_N$ are not isomorphic in this case. Conversely, consider $u \in \mathbb{Z}_n^\times$ arbitrary, and let $(u_M, u_N) = \rho(u)$. If $-1 \in Q_M$, let $i \in \mathbb{Z}_M$ such that $i^2 = -1$: for any $s_M, s_N \in \{0, 1\}$, we then have

$$\begin{aligned}\Big((-1)^{s_M} u_M^2,\, (-1)^{s_N} u_N^2\Big) &= (-1)^{s_N}\Big((-1)^{s_M - s_N} u_M^2,\, u_N^2\Big) \\ &= (-1)^{s_N}\Big(\big[i^{(s_M - s_N)} u_M\big]^2,\, u_N^2\Big). \qquad (1)\end{aligned}$$

Thus $T_M \oplus T_N \leqslant \sigma(T_{MN})$; and similarly if $-1 \in Q_N$. □

**Remark.** The above result is similar to [8, Theorem 8], which uses a "partial transpose" criterion to indicate when a graph may be regarded as a symmetric difference of tensor products of graphs on $M$ and $N$ vertices; the presence of $-1$ in either $Q_M$ or $Q_N$ is equivalent to $G_{MN}$ being invariant under partial transposes (w.r.t. to the tensor decomposition induced by $\rho$).

**Corollary 1-1.** *For $n \geqslant 1$, let $n = p_1^{m_1} \cdots p_\tau^{m_\tau} N$ be a factorization of $n$ such that $p_j \equiv 1 \pmod 4$ for each $1 \leqslant j \leqslant \tau$, and $N$ has no such prime factors. Then $G_n \cong G_{p_1{}^{m_1}} \otimes \cdots \otimes G_{p_\tau{}^{m_\tau}} \otimes G_N$ .*

*Proof.* For $p_j$ odd, $\mathbb{Z}^\times_{p_j{}^{m_j}}$ is a cyclic group [7] of order $(p_j - 1)p_j^{m_j - 1}$ in which $-1$ is the unique element of order two: then $-1$ is a quadratic residue modulo $p_j^{m_j}$ if and only if $p_j \equiv 1 \pmod 4$. As this holds for all $1 \leqslant j \leqslant \tau$, repeated application of Theorem 1 yields the decomposition above. □

**Corollary 1-2.** *For $n \geqslant 1$, we have $G_n \cong G_{p_1{}^{m_1}} \otimes \cdots \otimes G_{p_t{}^{m_t}}$ if and only if either $n$ has at most one prime factor $p_j \not\equiv 1 \pmod 4$, or $n$ has two such factors and $n \equiv 2 \pmod 4$.*

*Proof.* Suppose that $G_n$ decomposes as above. Let $N$ be the largest factor of $n$ which does not have prime factors $p \equiv 1 \pmod 4$: we continue from the proof of Corollary 1-1. By Theorem 1, $G_N$ itself decomposes as a tensor factor over its prime power factors $p_{\tau+1}^{m_{\tau+1}}, \ldots, p_t^{m_t}$ if and only if there is at most one such prime $p_j$ such that $-1 \notin Q_{p_j{}^{m_j}}$. However, by construction, all odd prime factors $p_j$ of $N$ satisfy $p_j \equiv 3 \pmod 4$, in which case $-1 \notin Q_{p_j{}^{m_j}}$ for any of them. Furthermore, for $m \geqslant 2$, we have $r \in Q_{2^m}$ only if $r \equiv 1 \pmod 4$; then $-1 \in Q_{2^m}$ if and only if $2^m = 2$. Thus, if $G_n \cong G_{p_1{}^{m_1}} \otimes \cdots \otimes G_{p_t{}^{m_t}}$, it follows either that $N = p^m$ for some prime $p \equiv 3 \pmod 4$, in which case the decomposition of Corollary 1-1 is the desired decomposition, or $N = 2p^m$ for some prime $p \equiv 3 \pmod 4$, in which case $n \equiv 2 \pmod 4$. The converse follows easily from Corollary 1-1 and Theorem 1. □

We finish our discussion of tensor products with an observation for prime powers. Let $\mathring{K}_M$ denote the complete pseudograph on $M$ vertices (*i.e.* an $M$-clique with loops):

**Lemma 2.** *For $m \geqslant 3$, we have $G_{2^m} \cong G_8 \otimes \mathring{K}_{2^{m-3}}$ and $\Gamma_{2^m} \cong \Gamma_8 \otimes \mathring{K}_{2^{m-3}}$; for $p$ an odd prime and $m \geqslant 1$, we have $G_{p^m} \cong G_p \otimes \mathring{K}_{p^{m-1}}$ and $\Gamma_{p^m} \cong \Gamma_p \otimes \mathring{K}_{p^{m-1}}$.*

*Proof.* We prove the results for $\Gamma_{p^m}$; the results for $G_{p^m}$ are similar.

- Let $n = 2^m$ for $m \geqslant 3$. We have $q \in Q_n$ if and only if $q \equiv 1 \pmod 8$. Let $\tau : \mathbb{Z}_{2^m} \to \mathbb{Z}_8 \times \mathbb{Z}_{2^{m-3}}$ (not a ring homomorphism) be defined by $\tau(r) = (r', k')$ such that $r = 8k' + r'$ for $r' \in \{0, \ldots, 7\}$. Then, we have $a - b \in Q_n$ if and only if $\tau(a - b) \in \{1\} \times \mathbb{Z}_{2^{m-3}}$, so that $\tau$ induces a homomorphism $\Gamma_n \cong \Gamma_8 \otimes \mathring{K}_{2^{m-3}}$.

- Similarly, for $n = p^m$ for $p$ an odd prime and $m \geqslant 1$, we have $q = pk' + q' \in Q_n$ (for $q' \in \{0, \ldots, p-1\}$, which we we identify with $\mathbb{Z}_p$) if and only if $q' \in Q_p$. If $\tau : \mathbb{Z}_{2^m} \to \mathbb{Z}_p \times \mathbb{Z}_{p^{m-1}}$ is defined by $\tau(q) = (q', k')$, we then have $a - b \in Q_n$ if and only if $\tau(a - b) \in Q_p \times \mathbb{Z}_{p^{m-1}}$. Thus, $\tau$ induces a homomorphism $\Gamma_n \cong \Gamma_p \otimes \mathring{K}_{p^{m-1}}$. □

Together with Corollary 1-1, and the fact that $\mathring{K}_{p^m}$ itself may be decomposed for any prime $p$ as an $m$-fold tensor product $\mathring{K}_p \otimes \cdots \otimes \mathring{K}_p$, the graph $G_n$ may be decomposed very finely whenever $n$ is dominated by prime-power factors $p^m$ for $p \equiv 1 \pmod 4$.

# 3 Induced paths and cycles of $G_n$

Even when the graph $G_n$ does not itself decompose as a tensor product, we may fruitfully describe such properties as walks in the graphs $G_n$ in terms of correlated transitions in tensor-factor "subsystems". This intuition will guide the analysis of this section in our characterization both of the diameters of the graphs $G_n$, and of the factors of $n$ for $G_n$ a perfect graph.

As $T_n$ is a multiplicative subgroup of $\mathbb{Z}_n^\times$, we may easily show that the graphs $G_n$ are arc-transitive. For any pair of edges $vw, v'w' \in E(G_n)$, the affine function $f(x) = (w' - v')(w - v)^{-1}(x - v) + v'$ is an automorphism of $G_n$ which maps $v \mapsto v'$ and $w \mapsto w'$. Consequently $G_n$ is vertex-transitive as well, so that we may bound the diameter by bounding the distance of vertices $v \in V(G)$ from $0 \in V(G)$, and also restrict our attention to odd induced cycles (or *odd holes*) which include 0 in our analysis of perfect graphs.

Let $A_n$, $B_n$ be the adjacency graphs of the graph $G_n$ and the digraph $\Gamma_n$ respectively. We then have $A_n = B_n = B_n^\top$ if and only if $-1$ is a quadratic residue modulo $n$, and $A_n = B_n + B_n^\top$ otherwise; in either case, we have $A_n \propto B_n + B_n^\top$. As $B_n$ may be decomposed as a Kronecker product (corresponding to the tensor decomposition of $\Gamma_n$), this suggests an analysis of walks in $G_n$ in terms of "synchronized walks" in the rings $\mathbb{Z}_{p_j^{m_j}}$ by adding or subtracting quadratic units, where one must add a quadratic unit in all rings simultaneously or subtract a quadratic unit in all rings simultaneously. This will inform the analysis of properties such as the diameters and perfectness of the graphs $G_n$.

## 3.1 Characterizing paths of length two for $n$ odd

To facilitate the analysis of this section, we will be interested in enumerating paths of length two in $G_n$ between distinct vertices. Because $A_n \propto B_n + B_n^\top$ for all $n$, we have

$$\begin{aligned} A_n^2 \;&\propto\; B_n^2 \,+\, 2B_nB_n^\top \,+\, \left(B_n^\top\right)^2 \\ &\cong\; \left[\bigotimes_{j=1}^{t} B_{p_j{}^{m_j}}^2\right] \,+\, 2\left[\bigotimes_{j=1}^{t} B_{p_j{}^{m_j}} B_{p_j{}^{m_j}}^\top\right] \,+\, \left[\bigotimes_{j=1}^{t} \left(B_{p_j{}^{m_j}}^\top\right)^2\right], \end{aligned} \tag{2}$$

where congruence is up to a permutation of the standard basis. Thus, we may characterize the paths of length two in $G_n$ between distinct vertices $r, s \in \mathbb{Z}_n$ in terms of the number of ways that we may represent $s - r$ in the form $\alpha^2 + \beta^2$, $\alpha^2 - \beta^2$, and $-\alpha^2 - \beta^2$ for some units $\alpha, \beta \in \mathbb{Z}_n^\times$; and these we may characterize in terms of products over the number of representations in the special case where $n$ is a prime power.

**Definition II.** For $n > 0$ and $r \in \mathbb{Z}_n$, we let $S_n(r)$ denote the number of solutions $(x, y) \in Q_n \times Q_n$ to the equation $r = x + y$; similarly, $D_n(r)$ denotes the number of solutions $(x, y) \in Q_n \times Q_n$ to the equation $r = x - y$.

Thus, when $-1 \in Q_n$ and $A_n = B_n = \frac{1}{2}(B_n + B_n^\top)$, the number of paths of length two from 0 to $r \neq 0$ is $S_n(r)$; otherwise, if $-1 \notin Q_n$, the number of such paths is $S_n(r) + 2D_n(r) + S_n(-r)$. Thus, the number of paths of length two from 0 to $r$ reduces to avaluation of the functions $S_n$ and $D_n$. We may evaluate these functions for $n$ a prime power, through a straightforward generalization of standard results on patterns of quadratic residues and non-residues to prime power moduli:

**Lemma 3.** *For $p$ a prime and $m \geqslant 1$, let $C_{p^m}^{++}$ (respectively $C_{p^m}^{--}$) denote the number of consecutive pairs of quadratic units (resp. consecutive pairs of non-quadratic units) modulo $p^m$, and $C_{p^m}^{+-}$ (respectively $C_{p^m}^{-+}$) denote the number of sequences of a quadratic unit followed by a non-quadratic unit (resp. a non-quadratic unit followed by a quadratic unit) modulo $p^m$. For primes $p \equiv 1 \pmod 4$, we have*

$$C_{p^m}^{++} = \frac{(p-5)p^{m-1}}{4}, \qquad C_p^{+-} = C_p^{-+} = C_p^{--} = \frac{(p-1)p^{m-1}}{4}; \tag{3a}$$

*otherwise, if $p \equiv 3 \pmod 4$, we have*

$$C_p^{+-} = \frac{(p+1)p^{m-1}}{4}, \qquad C_p^{++} = C_p^{-+} = C_p^{--} = \frac{(p-3)p^{m-1}}{4}. \tag{3b}$$

*Proof.* As $r \in \mathbb{Z}$ is a quadratic residue, quadratic non-residue, and/or unit modulo $p^m$ if and only the same properties hold modulo $p$, the distribution of quadratic and non-quadratic units modulo $p^m$ is simply that of the integers modulo $p$, repeated $p^{m-1}$ times. It then suffices to multiply the formulae given for $C_p^{++}$, $C_p^{+-}$, $C_p^{-+}$, $C_p^{--}$ (obtained by Aladov [9]) by $p^{m-1}$. □

**Lemma 4.** *Let $p$ be an odd prime, $m > 0$, and $r \in \mathbb{Z}_{p^m}$. If $p \equiv 1 \pmod 4$, we have*

$$S_{p^m}(r) = D_{p^m}(r) = \begin{cases} \frac{1}{4}(p-5)p^{m-1}, & \text{for } r \text{ a quadratic unit,} \\ \frac{1}{4}(p-1)p^{m-1}, & \text{for } r \text{ a non-quadratic unit,} \\ \frac{1}{2}(p-1)p^{m-1}, & \text{for } r \text{ a zero divisor;} \end{cases} \tag{4a}$$

*for $p \equiv 3 \pmod 4$, we instead have*

$$S_{p^m}(r) = \begin{cases} \frac{1}{4}(p-3)p^{m-1}, & \text{for } r \text{ a quadratic unit,} \\ \frac{1}{4}(p+1)p^{m-1}, & \text{for } r \text{ a non-quadratic unit,} \\ 0, & \text{for } r \text{ a zero divisor;} \end{cases} \tag{4b}$$

$$D_{p^m}(r) = \begin{cases} \frac{1}{4}(p-3)p^{m-1}, & \text{for } r \text{ a unit,} \\ \frac{1}{2}(p-1)p^{m-1}, & \text{for } r \text{ a zero divisor.} \end{cases} \tag{4c}$$

*Proof.* We proceed by cases, according to whether $r$ is a quadratic unit, non-quadratic unit, or zero modulo $p$:

- Suppose $r \in Q_n$. Each consecutive pair $q, q+1 \in Q_{p^m}$ yields a solution $(x, y) = (r(q+1), rq) \in Q_{p^m} \times Q_{p^m}$ to $x - y = r$; then we have $D_{p^m}(r) = C^{++}_{p^m}$. Similarly, each such pair yields a solution $(x, y) = (rq(q+1)^{-1}, r(q+1)^{-1}) \in Q_{p^m} \times Q_{p^m}$ to $x + y = r$; then $S_{p^m}(r) = C^{++}_{p^m}$ as well.

- Suppose $r \in \mathbb{Z}^\times_{p^m} \setminus Q_{p^m}$. Each consecutive pair $s, s+1 \in \mathbb{Z}^\times_{p^m} \setminus Q_{p^m}$ represents a solution in non-quadratic units to $x - y = 1$; these may then be used to obtain solutions $(rx, ry) \in Q_{p^m} \times Q_{p^m}$ to $rx - ry = r$, so that $D_{p^m}(r) = C^{--}_{p^m}$. In the case that $p \equiv 1 \pmod 4$, the negation of a quadratic unit is also a quadratic unit; in this case, we have the same number of solutions $(rx, -ry) \in Q_{p^m} \times Q_{p^m}$ to $rx + (-ry) = r$, so that $S_{p^m}(r) = C^{--}_{p}$ as well.

  If instead $p \equiv 3 \pmod 4$, we instead consider quadratic units $s \in Q_{p^m}$ such that $s+1$ is a non-quadratic unit. Each such pair yields a solution $(x, y) = (r(s+1), -rs) \in Q_{p^m} \times Q_{p^m}$ to $x + y = r$; then we have a solution for each such pair $s, s+1$, so that $S_{p^m}(r) = C^{+-}_{p^m}$.

- Finally, suppose $r$ is a multiple of $p$. The congruence $x + y \equiv 0 \pmod p$ is satisfiable for $(x, y) \in Q_{p^m} \times Q_{p^m}$ only if $-x$ is a quadratic unit modulo $p$ for some $x \in Q_{p^m}$, *i.e.* if $p \equiv 1 \pmod 4$. If this is the case, then every $x \in Q_{p^m}$ contributes a solution $(x, y) = (x, r - x) \in Q_{p^m} \times Q_{p^m}$ to $x + y = r$; otherwise, in the case $p \equiv 3 \pmod 4$, there are no solutions. Similarly, regardless of the value of $p$, each quadratic unit $x \in Q_{p^m}$ contributes a solution $(x, y) = (x, x - r) \in Q_{p^m} \times Q_{p^m}$ to $x - y = r$. Thus $D_{p^m}(r) = \frac{1}{2}(p-1)$ for all $p$; $S_{p^m}(r) = \frac{1}{2}(p-1)$ for $p \equiv 1 \pmod 4$; and $S_{p^m}(r) = 0$ for $p \equiv 3 \pmod 4$. □

**Corollary 4-1.** $\operatorname{diam}(G_{p^m}) \leqslant 2$ *for* $p$ *an odd prime and* $m > 0$*; this inequality is strict if and only if* $p \equiv 3 \pmod 4$ *and* $m = 1$.

*Proof.* Clearly for $p \equiv 1 \pmod 4$ we have $\operatorname{diam}(G_{p^m}) = 2$; suppose then that $p \equiv 3 \pmod 4$. We may form any zero divisor $s = pk$ as a difference of quadratic units $x \in Q_{p^m}$ and $x - pk \in Q_{p^m}$, so that $\operatorname{diam}(G_{p^m}) \leqslant 2$. We have $\operatorname{diam}(G_{p^m}) = 1$ only if 0 is the only zero divisor of $\mathbb{Z}_{p^m}$; this implies that $m = 1$, in which case $T_{p^m} = \mathbb{Z}_p^\times$, so that the converse also holds. □

In Lemma 4, $n = 3^m$ and $n = 5^m$ are cases for which there do not exist paths of length two from zero to any quadratic unit. This does not affect the diameters of the graphs $G_{3^m}$ or $G_{5^m}$ for $m > 0$; however, using the following Lemma, we shall see that this deficiency affects the diameters of $G_n$ for any other $n$ a multiple of either 3 or 5.

**Lemma 5.** *For* $n > 0$ *odd and* $r \in \mathbb{Z}_n$*, we have* $S_n(r) = 0$ *if and only if at least one of the following conditions hold:*

(*i*) $n$ *is a multiple of* 3*, and* $r \not\equiv 2 \pmod 3$*;*

(*ii*) $n$ *is a multiple of* 5*, and* $r \equiv \pm 1 \pmod 5$*; or*

(*iii*) $n$ *has a prime factor* $p_j \equiv 3 \pmod 4$ *such that* $r \in p_j\mathbb{Z}_n$.

*Similarly, we have* $D_n(r) = 0$ *if and only if at least one of the following conditions hold:*

(*i*) $n$ *is a multiple of* 3*, and* $r \not\equiv 0 \pmod 3$*; or*

(*ii*) $n$ *is a multiple of* 5*, and* $r \equiv \pm 1 \pmod 5$.

*Proof.* For $r \in \mathbb{Z}_n$ arbitrary, let $(r_1, r_2, \ldots, r_t) = \sigma(r)$. By the decompositions $B_n^2 \cong B_{p_1^{m_1}}^2 \otimes \cdots \otimes B_{p_t^{m_t}}^2$ and $B_n B_n^\top \cong B_{p_1^{m_1}} B_{p_1^{m_1}}^\top \otimes \cdots \otimes B_{p_t^{m_t}} B_{p_t^{m_t}}^\top$, we may express $S_n(r)$ and $D_n(r)$ as products over the prime-power factors of $n$,

$$S_n(r) \;=\; \prod_{j=1}^{t} S_{p_j^{m_j}}(r_j)\;, \qquad\qquad D_n(r) \;=\; \prod_{j=1}^{t} D_{p_j^{m_j}}(r_j)\;. \tag{5}$$

These are zero if and only if there exist $1 \leqslant j \leqslant t$ such that $S_{p_j^{m_j}}(r_j) = 0$ or $D_{p_j^{m_j}}(r_j) = 0$, respectively. By Lemma 4, $S_{p_j^{m_j}}(r_j) = 0$ if and only if either $r_j$ is a zero divisor of $\mathbb{Z}_{p_j^{m_j}}$ for a prime factor $p_j \equiv 3 \pmod 4$, or if $p_j \in \{3, 5\}$ and $r_j$ is a quadratic unit modulo $\mathbb{Z}_{p_j^{m_j}}$; similarly, $D_{p_j^{m_j}}(r_j) = 0$ if and only if $p_j = 3$ and $r_j$ is a unit modulo 3, or $p_j = 5$ and $r_j$ is a quadratic unit modulo 5. □

## 3.2 Diameter of $G_n$ for odd $n$

For odd integers $n$, characterizing the diameters of $G_n$ involves accounting for "problematic" prime factors of $n$ (those described in Lemma 5), which present obstacles to the construction of short paths between distinct vertices:

**Theorem 6.** *Let $n > 1$ odd. Let $\gamma_3(n) = 1$ if $n$ is a multiple of 3, and $\gamma_3(n) = 0$ otherwise; $\delta_3(n) = 1$ if $n$ has prime factors $p_j \equiv 3 \pmod 4$ for $p_j > 3$, and $\delta_3(n) = 0$ otherwise; and $\gamma_5(n) = 1$ if $n$ is a multiple of 5, and $\gamma_5(n) = 0$ otherwise. Then, we have*

$$\operatorname{diam}(G_n) = \begin{cases} 1, & \text{if } n \text{ is prime and } n \equiv 3 \pmod 4; \\ 2, & \text{if } n \text{ is prime and } n \equiv 1 \pmod 4; \\ 2, & \text{if } \omega(n) = 1 \text{ and } n \text{ is composite}; \\ 2 + \gamma_3(n)\delta_3(n) + \gamma_5(n), & \text{if } \omega(n) > 1. \end{cases}$$

*In particular,* $\operatorname{diam}(G_n) \leqslant 4$.

*Proof.* The diameters for $\omega(n) = 1$ are characterized by Corollary 4-1: we thus restrict ourselves to the case $\omega(n) > 1$.

We have $\operatorname{diam}(G_n) \leqslant 2$ if and only if either $S_n(r)$, $S_n(-r)$, or $D_n(r)$ is positive for all $r \in \mathbb{Z}_n \smallsetminus T_n$. By Lemma 5, $D_n(r) > 0$ for all $r \in \mathbb{Z}_n$ if $n$ is relatively prime to 15; then $\operatorname{diam}(G_n) = 2$, and $r = u - u'$ for some $u, u' \in Q_n$ for any $r \in \mathbb{Z}_n$ if $\gamma_3 = \gamma_5 = 0$. If $n$ is a multiple of 5, however, we have $S_n(r) = S_n(-r) = D_n(r) = 0$ for any non-quadratic unit $r \equiv \pm 1 \pmod 5$, of which there is at least one (as $n$ is not a power of 5): thus $\operatorname{diam}(G_n) \geqslant 3$ if $\gamma_5(n) = 1$.

Suppose that $n$ is relatively prime to 5, and is a multiple of 3. Again by Lemma 5, there are walks of length two from 0 to $r$ if $r \equiv 0 \pmod 3$, as we have $D_n(r) > 0$ in this case. However, if $n$ has prime factors $p_j > 3$ such that $p_j \equiv 3 \pmod 4$, there exist $r \in p_j\mathbb{Z}_n$ such that $r \not\equiv 0 \pmod 3$, in which case we have $S_n(r) = S_n(-r) = D_n(r) = 0$. Thus, if $\gamma_3(n) = \delta_3(n) = 1$, we have $\operatorname{diam}(G_n) \geqslant 3$. Otherwise, if $\delta_3(n) = 0$, we have either $S_n(r) > 0$ in the case that $r \equiv 2 \pmod 3$, or $S_n(-r) > 0$ in the case that $r \equiv 1 \pmod 3$. In this case, every vertex $r \neq 0$ is reachable by a path of length two, so that $\operatorname{diam}(G_n) = 2$ if $\gamma_3(n) = 1$ and $\delta_3(n) = \gamma_5(n) = 0$.

Finally, suppose that either $\gamma_5(n) = 1$ or $\gamma_3(n) = \delta_3(n) = 1$: from the analysis above, we have $\operatorname{diam}(G_n) \geqslant 3$. For $r \in \mathbb{Z}_n$, let $(r_1, \ldots, r_n) = \sigma(r)$, where we arbitrarily label $p_3 = 3$ if $n$ is a multiple of 3, and $p_5 = 5$ if $n$ is a multiple of 5. We may then classify the distance of $r \in V(G_n)$ away from zero, as follows.

- Suppose that $n$ is a multiple of 3 and some other $p_j \equiv 3 \pmod 4$, and that either $n$ is relatively prime to 5 or $r \not\equiv \pm 1 \pmod 5$. By Lemma 5, we have $D_n(r) > 0$ if $r \equiv 0 \pmod 3$, in which case it is at a distance of two from 0. Otherwise, for $r \equiv \pm 1 \pmod 3$, let $s = r \mp u$ for $u \in Q_n$: then $s \equiv 0 \pmod 3$. Then $D_n(s) > 0$, in which case $r = u'' - u' \pm u$ for some choice of units $u', u'' \in Q_n$, so that $r$ can be reached from 0 by a walk of length three.

- Suppose that $n$ is a multiple of 5 and that $r \not\equiv 0 \pmod 5$. We may select coefficients $u_j \in Q_{{p_j}^{m_j}}$ such that $r_5 - u_5 \in \{2, 3\}$, and such that $u_j \neq r_j$ for any $p_j \geqslant 7$. Let $u = \sigma^{-1}(u_1, \ldots, u_t)$: by construction, we then have $r - u \equiv \pm 2 \pmod 5$ and $r - u \not\equiv 0 \pmod{p_j}$ for $p_j \geqslant 7$. Then either $S_n(r - u) > 0$, $S_n(u - r) > 0$, or $D_n(r - u) > 0$ (according to whether or not $n$ is a multiple of 3, and which residue $r$ has modulo 3 if so): $r$ can then be reached from 0 by a path of length three.

- Suppose that $n$ is a multiple of 5, and that $r \equiv 0 \pmod 5$. If $n$ is not a multiple of 3, or if $r \equiv 0 \pmod 3$, then $D_n(r) > 0$; $r$ can then be reached from 0 by a walk of length two. We may then suppose that $n$ is a multiple of 3 and $r \equiv \pm 1 \pmod 3$. If we also have $r \not\equiv 0 \pmod{p_j}$ for any $p_j \equiv 3 \pmod 4$, one of $S_n(r)$ or $S_n(-r)$ is non-zero; again, $r$ is at a distance of two from 0. Otherwise, we have $r \equiv 0 \pmod{p_j}$ for any $p_j \equiv 3 \pmod 4$, so that $S_n(r) = S_n(-r) = D_n(r) = 0$; then $r$ has a distance at least three from 0. As well, any neighbor $s = r \pm u$ (for $u \in Q_n$ arbitrary) satsifies $s \equiv \pm 1 \pmod 5$. Then each neighbor of $r$ is then at distance three from 0 in $G_n$, from which it follows that $r$ is at a distance of four from 0.

Thus, there exist vertices at distance four from 0 if $\gamma_3(n)\delta_3(n)+\gamma_5(n) = 2$; and apart from these vertices, or in the case that $\gamma_3(n)\delta_3(n)+\gamma_5(n) = 1$, each vertex is at a distance of at most three from 0. Then $\operatorname{diam}(G_n) = 2+\gamma_3(n)\delta_3(n)+\gamma_5(n)$ if $\omega(n) > 1$, as required. □

## 3.3 Restricted reachability results for $n$ coprime to 6

We may prove some stronger results on the reachability of vertices from 0 in $G_n$ for $n$ odd: this will facilitate the analysis of perfectness results and the diameters for $n$ even.

**Definition III.** For a (di-)graph $G$, the *uniform diameter* $\operatorname{udiam}(G)$ is the minimum integer $d$ such that, for any two vertices $v, w \in V(G)$, there exists a (directed) walk of length $d$ from $v$ to $w$ in $G$.

Our interest in "uniform" diameters is due to the fact that if every vertex $v \in V(\Gamma_n)$ can be reached from 0 by a path of exactly $d$ in $\Gamma_n$, then $v$ can also be reached from 0 by a path of any length $\ell \geqslant d$ as well, which will prove useful for describing walks in $\Gamma_n$ to arbitrary vertices in terms of simultaneous walks in the digraphs $\Gamma_{p_j{}^{m_j}}$.

We may easily show that $\Gamma_n$ has no uniform diameter when $n$ is a multiple of 3. For any adjacent vertices $v$ and $w$ such that $w - v \in Q_n$, we have $w - v \equiv 1 \pmod 3$ by that very fact. Then, there is a walk of length $\ell$ from $v$ to $w$ only if $\ell \equiv 1 \pmod 3$; similarly, there is a walk of length $\ell$ from $w$ to $v$ only if $\ell \equiv 2 \pmod 3$. For similar reasons, $\Gamma_n$ has no uniform diameter for $n$ even. However, for $n$ relatively prime to 6, $\Gamma_n$ has a uniform diameter which may be easily characterized:

**Theorem 7.** *Let $n = p_1^{m_1} \cdots p_t^{m_t}$ be relatively prime to 6. Then*

$$\operatorname{udiam}(\Gamma_n) = \begin{cases} 2\,, & \text{if } n \text{ is coprime to } 5 \text{ and } \forall j : p_j \equiv 1 \pmod 4; \\ 3\,, & \text{if } n \text{ is coprime to } 5 \text{ and } \exists j : p_j \equiv 3 \pmod 4; \\ 4\,, & \text{if } n \text{ is a multiple of } 5. \end{cases}$$

*Proof.* We begin by characterizing $\operatorname{udiam}(\Gamma_n)$, where $n = p^m$ for $p \geqslant 5$ prime, using Lemma 4 throughout to characterize $S_n(r)$ for $r \in \mathbb{Z}_n$.

- If $p \equiv 1 \pmod 4$ and $p > 5$, we have $S_{p^m}(r) > 0$ for all $r \in \mathbb{Z}_n$; then $\operatorname{udiam}(\Gamma_n) = 2$.

- If $p \equiv 3 \pmod 4$ and $p > 5$, we have $S_{p^m}(r) = 0$ if and only if $r \in \mathbb{Z}_n$ is a zero divisor. In particular, $\operatorname{udiam}(\Gamma_n) \geqslant 3$. Conversely, as $\left|\mathbb{Z}_{p^m}^\times\right| > p^{m-1}$, there exists $z \in Q_{p^m}^\times$ such that $r - z$ is a unit; then there are quadratic units $x, y \in Q_{p^m}$ such that $r - z = x + y$, so that $\operatorname{udiam}(\Gamma_n) = 3$.

- If $p = 5$, we have $u \in Q_{5^m}$ if and only if $u \equiv \pm 1 \pmod 5$; then $r$ can be expressed as a sum of $k$ quadratic units $r = u_1 + \cdots + u_k$ if and only if $r$ can be expressed modulo 5 as a sum or difference of $k$ ones; that is, if $r \in \{-k, -k+2, \ldots, k-2, k\} + 5\mathbb{Z}_{5^m}$ (which exhausts $\mathbb{Z}_{5^m}$ for $k \geqslant 4$).

For $n$ not a prime power, we decompose $\Gamma_n \cong \Gamma_{p_1{}^{m_1}} \otimes \cdots \otimes \Gamma_{p_t{}^{m_t}}$; then a vertex $r = \sigma^{-1}(r_1, \ldots, r_t)$ is reachable by a walk of length $\ell$ in $\Gamma_n$ if and only if each $r_j \in V(\Gamma_{p_j{}^{m_j}})$ are reachable by such a walk in their respective digraphs. Thus, the uniform diameter of the tensor product is the maximum of the uniform diameters of each factor. □

The uniform diameter $\Gamma_n$ happens also to provide an upper bound on distances between vertices in $G_n$, under the constraint that we may only traverse walks $w_0\, w_1 \ldots w_\ell$ where the "type" of each transition $w_j \to w_{j+1}$ is fixed to be either a quadratic unit or the negation of a quadratic unit, independently for each $j$. More precisely:

**Lemma 8.** *Let $n = p_1^{m_1} \cdots p_t^{m_t}$ be relatively prime to 6, and $\ell \geqslant \operatorname{udiam}(\Gamma_n)$. For any sequence $s_1, \ldots, s_\ell \in \{0, 1\}$, these exists a sequence of quadratic units $u_1, \ldots, u_\ell \in Q_n$ such that $r = (-1)^{s_1} u_1 + (-1)^{s_2} u_2 + \cdots + (-1)^{s_\ell} u_\ell$.*

*Proof.* We first show that there are solutions to $r = u_1 - u_2 \pm u_3 \pm \cdots \pm u_\ell$, where all but the first two signs may be arbitrary. We prove the result for $\ell = \operatorname{udiam}(\Gamma_n)$; one may extend to $\ell > \operatorname{udiam}(\Gamma_n)$ by induction.

- Suppose $n$ is coprime to 5: then for any $r \in \mathbb{Z}_n$, we have $D_n(r) > 0$, so that there exist $u, u' \in Q_n$ such that $r = u - u'$. In the case that $n$ also has prime factors $p_j \equiv 3 \pmod 4$, consider $s = r \mp u$ for any $u \in Q_n$: as there are solutions to $s = u - u'$ for $u, u' \in Q_n$, there are also solutions to $r = u - u' \pm u''$.

- Suppose $n = 5^{m_1} p_2^{m_2} \cdots p_t^{m_t}$.

  - If $r \not\equiv \pm 1 \pmod 5$. Let $s \in \mathbb{Z}_n$ be such that $s \equiv 0 \pmod 5$, and $s \not\equiv 0 \pmod{p_j}$ for any $p_j \geqslant 7$. Then $r - s \not\equiv \pm 1 \pmod 5$, so that $D_n(r) > 0$; by Lemma 5, there are then quadratic units $u_1, u_2 \in Q_n$ such that $r - s = u_1 - u_2$. We also have $S_n(s), S_n(-s), D_n(s) > 0$ by construction, which can be used to obtain decompositions $s = \pm u_3 \pm u_4$ for $u_3, u_4 \in Q_n$ depending on the choices of signs; we then have $r = u_1 - u_2 \pm u_3 \pm u_4$.
  - If $r \equiv \pm 1 \pmod 5$, consider $(r_1, \ldots, r_t) = \sigma(r)$. We select coefficients $u_j, u_j' \in Q_{p_j{}^{m_j}}$ as follows. We set $u_1' = -u_1 = r_1$, so that

$$(r_1 - 2u_1) \equiv (r_2 + 2u_2') \equiv (r_1 - u_1 + u_1') = \pm 3 \pmod 5. \tag{6a}$$

For each $p_j \geqslant 7$, we require $u_j \neq 2^{-1}r_j$ and $u'_j \notin \{-2^{-1}r_j,\, u_j - r_j\}$, but may otherwise leave $u_j$ unconstrained; we then have

$$(r_j - 2u_j),\, (r_j + 2u'_j),\, (r_j - u_j + u'_j) \neq 0 \qquad \text{for } p_j \geqslant 7. \tag{6b}$$

Let $u = \sigma^{-1}(u_1, \ldots, u_t)$ and $u' = \sigma^{-1}(u'_1, \ldots, u'_t)$. By construction, we then have $D_n(r - 2u), D_n(r + 2u'), D_n(r - u + u') > 0$ by Lemma 5. There then exist $u'', u''' \in Q_n$ such that

$$r = u''' - u'' + u + u\,, \quad \text{or} \tag{7a}$$
$$r = u''' - u'' + u - u' = u''' - u'' - u' + u\,, \quad \text{or} \tag{7b}$$
$$r = u''' - u'' - u' - u'\,, \tag{7c}$$

selecting $u'', u'''$ according to the desired signs for the latter two terms.

Thus, there are solutions to $r = u_1 - u_2 \pm u_3 \pm \cdots \pm u_\ell$ for $u_j \in Q_n$ and $\ell = \operatorname{udiam}(\Gamma_n)$, for arbitrary choices of signs and $r \in \mathbb{Z}_n$. It follows that we may decompose $r = \pm u_1 \pm \cdots \pm u_\ell$ for arbitrary choices of sign, provided not all signs are the same. By considering walks in $\Gamma_n$ of length $\operatorname{udiam}(\Gamma_n)$ from 0 to either $r$ or $-r$, we also have decompositions $r = u_1 + \cdots + u_\ell$ and $r = -u_1 - \cdots - u_\ell$ for suitable choices of $u_1, \ldots, u_\ell \in Q_n$. □

The principal motivation for Lemma 8 is to bound the diameters of graphs $G_n$ over tensor decompositions of the ring $\mathbb{Z}_n$:

**Lemma 9.** *Let $M, N \geqslant 1$ be relatively prime integers, and let $n = MN$. Then we have $\operatorname{diam}(G_n) \geqslant \max\{\operatorname{diam}(G_N), \operatorname{diam}(G_M)\}$. Furthermore, if $M$ is coprime to 6, we have $\operatorname{diam}(G_n) \leqslant \max\{\operatorname{diam}(G_N), \operatorname{udiam}(\Gamma_M) + 1\}$ as well.*

*Proof.* Let $\rho : \mathbb{Z}_n \longrightarrow \mathbb{Z}_N \oplus \mathbb{Z}_M$ be the natural isomorphism. Let $r \in \mathbb{Z}_n$ be arbitrary, and $(r', r'') = \rho(r)$. If $r = (-1)^{s_1}u_1 + \cdots + (-1)^{s_\ell}u_\ell$ for some $\ell > 0$ and $u_1, \ldots, u_\ell \in Q_n$, we also have

$$r' = (-1)^{s_1}\, u'_1 + \cdots + (-1)^{s_\ell}\, u'_\ell\,, \tag{8a}$$
$$r'' = (-1)^{s_1}\, u''_1 + \cdots + (-1)^{s_\ell}\, u''_\ell\,, \tag{8b}$$

where $(u'_j, u''_j) = \rho(u_j)$. For $\ell = \operatorname{diam}(G_n)$, it follows that $\ell \geqslant \operatorname{diam}(G_M)$ and $\ell \geqslant \operatorname{diam}(G_N)$.

Suppose further that $M$ is relatively prime to 6: then $\operatorname{udiam}(\Gamma_M)$ is well-defined by Lemma 8. For any $a \in \mathbb{Z}_N$, let $\ell > 0$ be the length of a walk in $G_N$ from 0 to $\ell$: there are then $u_1, \ldots, u_\ell \in Q_N$ and $s_1, \ldots, s_\ell \in \{0, 1\}$ such that $a = (-1)^{s_1}u'_1 + \cdots + (-1)^{s_\ell}u'_\ell$. If $\ell \geqslant \operatorname{udiam}(\Gamma_M)$, then for any $b \in \mathbb{Z}_M$, there also exist quadratic units $u''_1, \ldots, u''_\ell \in Q_M$ such that $b = (-1)^{s_1}u'''_1 + \cdots + (-1)^{s_\ell}u'''_\ell$. We may always obtain such a walk of length $\ell \geqslant \operatorname{udiam}(\Gamma_M)$ in $G_N$ by taking the shortest walk from 0 to $a$ in $G_N$, and repeatedly adding

closed walks of length two to the end until we obtain a walk of length $\ell \geqslant \operatorname{udiam}(\Gamma_M)$. For such a walk, we then have

$$\begin{aligned} r \;=\; \rho^{-1}(a,b) \;&= \rho^{-1}\left( \sum_{j=1}^{\ell} (-1)^{s_j} u'_j \;\;,\;\; \sum_{j=1}^{\ell} (-1)^{s_j} u''_j \right) \\ &= \sum_{j=1}^{\ell} (-1)^{s_j} \rho^{-1}(u'_j, u''_j) \;=\; \sum_{j=1}^{\ell} (-1)^{s_j} u_j \;, \end{aligned} \tag{9}$$

for some choice of quadratic units $u_j = \rho^{-1}(u'_j, u''_j) \in Q_n$ and $s_j \in \{0,1\}$. If $\operatorname{diam}(G_N) > \operatorname{udiam}(\Gamma_M)$, this construction yields path-lengths $\operatorname{udiam}(\Gamma_M) \leqslant \ell \leqslant \operatorname{diam}(G_N)$; if instead $\operatorname{udiam}(\Gamma_M) \geqslant \operatorname{diam}(G_N)$, we obtain paths of length at most $\operatorname{udiam}(\Gamma_M)+1$, which is saturated if there exist vertices $a \in V(G_N)$ whose distance $d_a$ from 0 is such that $\operatorname{udiam}(\Gamma_M) - d_a$ is odd. In either case, we have $\operatorname{diam}(G_n) \leqslant \max\{\operatorname{diam}(G_N), \operatorname{udiam}(\Gamma_M)+1\}$. □

## 3.4 Diameter of $G_n$ for $n$ even

The notable differences between the cases of $n$ odd and $n$ even are due to the sparsity of the quadratic units in $\mathbb{Z}_{2^m}$ compared to that of powers of other primes, and also that the sum or difference of two units (quadratic or otherwise) is necessarily a zero divisor if $n$ is even. This results in a significant increase of the maximum diameter in the case of $n$ even, compared to $n$ odd:

**Theorem 10.** *Let $n > 0$ even. Let $\delta_3(n) = 1$ if $n$ has prime factors $p_j \equiv 3 \pmod 4$ for $p_j > 3$, and $\delta_3(n) = 0$ otherwise. Then we have*

$$\operatorname{diam}(G_n) = \begin{cases} 12, & \text{if } n \text{ is a multiple of } 24; \\ 6, & \text{if } n \text{ is an odd multiple of } 12; \\ 5, & \text{if } n \text{ is a multiple of } 10, \text{ but not of } 12; \\ 4, & \text{if } n = 8K \text{ for } K > 0 \text{ coprime to } 15; \\ 3+\delta_3(n), & \text{if } n = 6K \text{ for } K > 0 \text{ coprime to } 10; \\ 3+\delta_3(n), & \text{if } n = 4K \text{ for } K > 1 \text{ coprime to } 30; \\ 3, & \text{if } n = 2K \text{ for } K > 1 \text{ coprime to } 30; \\ 2, & \text{if } n = 4; \\ 1, & \text{if } n = 2. \end{cases} \tag{10}$$

*In particular, with Theorem 6, we have $\operatorname{diam}(G_n) \leqslant 12$ for all $n$, and $\operatorname{diam}(G_{p^m}) \leqslant 4$ for any prime $p$ and $m \geqslant 0$.*

*Proof.* We use Lemma 9 to reduce the task of characterizing $\operatorname{diam}(G_n)$ for $n$ even to a small collection of representative cases, by factoring $n = NM$ for suitable choices of coprime factors $N$ and $M$.

- Suppose $n$ is a multiple of 12. We may let $M$ be the largest factor of $n$ which is coprime to 12, and $N = n/M$.
  - If $N = 2^m 3^{m'}$ for $m \geqslant 3$, we then have $u \in Q_N$ if and only if $u \equiv 1 \pmod 8$ and $u \equiv 1 \pmod 3$, or equivalently if $u \equiv 1 \pmod{24}$. Then $T_N$ consists of those $q \in \mathbb{Z}_N$ such that $r \equiv \pm 1 \pmod{24}$. The distance of a vertex in $G_N$ from 0 is then characterized by its residue modulo 24, in which case we may show that $\operatorname{diam}(G_N) = 12$.
  - Otherwise, $N = 4 \cdot 3^{m'}$, in which case $u \in Q_N$ if and only if $u \equiv 1 \pmod 4$ and $u \equiv 1 \pmod 3$, or equivalently if $u \equiv 1 \pmod{12}$. Then $T_N$ consists of those $q \in \mathbb{Z}_N$ such that $r \equiv \pm 1 \pmod{12}$; similarly as in the case above, we then have $\operatorname{diam}(G_N) = 6$.

  Because $\operatorname{diam}(G_M), \operatorname{udiam}(\Gamma_M) \leqslant 4$, we then have $\operatorname{diam}(G_n) = \operatorname{diam}(G_N)$ by Lemma 9. Thus $\operatorname{diam}(G_n) = 12$ if $N$ is a multiple of 24; otherwise we have $\operatorname{diam}(G_n) = 6$.

- Suppose $n$ is a multiple of 10, but not of 12: specifically, $n$ is not a multiple of 60. Let $M$ be the largest factor of $n$ which is coprime to 30, and $N = n/M$. We may show that $T_N$ contains only residues which are equivalent to $\pm 1$ modulo 10:
  - If $n$ is an odd multiple of 30, we have $N = 2 \cdot 3^m \cdot 5^{m'}$. Then $u \in Q_N$ if and only if $u$ is odd, $u \equiv 1 \pmod 3$, and $u \equiv \pm 1 \pmod 5$; equivalently, if $u \equiv 1 \pmod{30}$ or $u \equiv 19 \equiv -11 \pmod{30}$.
  - If $n$ is a multiple of 10 but not of 30, then without loss of generality $N = 2^{m_1} 5^{m_2}$. We may show that $r \in Q_N$ if and only if both $r \equiv \pm 1 \pmod 5$, and

$$r \equiv \begin{cases} 1 \pmod 2 & \text{if } m_1 = 1; \\ 1 \pmod 4 & \text{if } m_1 = 2; \\ 1 \pmod 8 & \text{if } m_1 \geqslant 3. \end{cases}$$

    In each case, we have $u \in Q_N$ if and only if $u \in \{1, 9\} \pmod{\bar{N}}$ for $\bar{N} = 10$, $\bar{N} = 20$, or $\bar{N} = 40$ respectively.

  As $N$ is a multiple of 10 in either case, vertices $r \in \mathbb{Z}_N$ such that $r \equiv 5 \pmod{10}$ can only be reached by a path from 0 with length at least five, so that $\operatorname{diam}(G_N) \geqslant 5$. We may show that this bound is tight by showing that every even residue can be formed as a sum of four elements of $T_n$. Let $x \equiv_m y$ denote equivalence of two integers (or sets of integers) modulo $m$. Then, we may easily verify that

$$\begin{aligned} \{\pm 1 \pm 1 \pm 1 \pm 1\} &\equiv_{30} \{26, 28, 0, 2, 4\}, \\ \{\pm 1 \pm 1 \pm 1 \pm 11\} &\equiv_{30} \{8, 10, 12, 14, 16, 18, 20, 22\}, \\ -11 - 11 - 1 - 1 &\equiv_{30} 6, \\ 11 + 11 + 1 + 1 &\equiv_{30} 24, \end{aligned} \tag{11a}$$

which proves the claim for $n$ an odd multiple of 30. For $n$ not a multiple of 30, $T_N$ is the set of elements $q \in \mathbb{Z}_N$ such that $q = 5 \pm 4 \pmod{\bar{N}}$ or $q = -5 \pm 4 \pmod{\bar{N}}$. It then suffices to show that all residues modulo 40 are exhausted by sums or differences of four such residues: we have

$$\begin{aligned}
\{\ (5 \pm 4) + (5 \pm 4) + (5 \pm 4) + (5 \pm 4)\ \} &\equiv_{40} \{4, 12, 20, 28, 36\}, \\
\{\ (5 \pm 4) + (5 \pm 4) + (5 \pm 4) - (5 \pm 4)\ \} &\equiv_{40} \{34,\ 2, 10, 18, 26\}, \\
\{\ (5 \pm 4) + (5 \pm 4) - (5 \pm 4) - (5 \pm 4)\ \} &\equiv_{40} \{24, 32,\ 0,\ 8, 16\}, \\
\{\ (5 \pm 4) - (5 \pm 4) - (5 \pm 4) - (5 \pm 4)\ \} &\equiv_{40} \{14, 22, 30, 38,\ 6\}.
\end{aligned} \tag{11b}$$

As every odd residue modulo $N$ is adjacent to an even residue, it follows that every vertex in $G_N$ can be reached by a path of length at most five; then $\operatorname{diam}(G_N) = 5$. As $M$ is coprime to both 3 and 5, we have $\operatorname{diam}(G_M) = 2$ and $\operatorname{udiam}(\Gamma_M) \leqslant 3$; thus $\operatorname{diam}(G_n) = 5$ by Lemma 9.

- Suppose that $n = 8K$ for $K$ coprime to 15. Let $M$ be the largest odd factor of $N$, and $N = n/M = 2^k$ for $k \geqslant 3$. By construction, $M$ is coprime to 6, so that $\operatorname{udiam}(\Gamma_M) \leqslant 3$. We have $u \in Q_N$ if and only if $u \equiv 1 \pmod 8$: as every odd residue modulo 8 can be expressed as a sum of three terms $\pm 1$, and every even residue modulo 8 can be expressed as a sum of four terms $\pm 1$ (with 4 requiring at least this many), it follows that $\operatorname{diam}(G_N) = 4$. By Lemma 9, it follows that $\operatorname{diam}(G_n) = 4$ as well.

- In the remaining cases, we either have $n = 2K$ for $K$ coprime to 15 and not a multiple of 4, or $n = 6K$ for $K$ coprime to 10. We trivially have $\operatorname{diam}(G_n) = \frac{n}{2}$ for $n \in \{2, 4\}$; otherwise, $n$ has odd zero divisors. As all walks of length one from 0 in $G_n$ end at quadratic units, and all walks of length two from 0 end at even elements of $\mathbb{Z}_n$, we require walks of length at least three from 0 to reach odd zero divisors in $\mathbb{Z}_n$. Thus, $\operatorname{diam}(G_n) \geqslant 3$.

  Let $M$ be the largest factor of $n$ which is coprime to 30. By construction, $M$ is coprime to 6, so that $\operatorname{udiam}(\Gamma_M) = 2 + \delta_3(M) = 2 + \delta_3(n)$.

  - If $n = 2K$ for $K$ coprime to 15 and not a multiple of 4, $M$ is simply the largest odd factor of $n$, in which case $n = 2^k$ for $k \in \{1, 2\}$. We then have $N \in \{2, 4\}$, so that $\operatorname{diam}(G_N) = \frac{1}{2}N \leqslant 2$.
  - If $n = 6K$ for $K$ coprime to 10, we have $N = 2 \cdot 3^k$ for some $k \geqslant 1$. Then $u \in Q_N$ if and only if $u \equiv 1 \pmod 3$ and is odd; that is, if $u \equiv 1 \pmod 6$. In particular, $T_N$ contains only elements which are equivalent to $\pm 1 \pmod 6$; from this we may easily show $\operatorname{diam}(G_N) = 3$.

  In either case, it follows by Lemma 9 that

$$3 \leqslant \operatorname{diam}(G_n) \leqslant \operatorname{udiam}(\Gamma_M) + 1 = 3 + \delta_3(n). \tag{12}$$

If $\delta_3(n) = 0$, we then have $\mathrm{diam}(G_n) = 3$; we may then restrict our attention to the case $\delta_3(n) = 1$.

Let $\rho : \mathbb{Z}_n \longrightarrow \mathbb{Z}_M \oplus \mathbb{Z}_N$ be the natural isomorphism. As $M$ is coprime to 15, we have $D_M(a) > 0$ for every $a \in \mathbb{Z}_M$ by Lemma 5: then we may express any $a \in \mathbb{Z}_M$ as a difference $a = u'_1 - u'_2$ for $u'_1, u'_2 \in Q_M$.

- If $N = 2$, any even residue $r$ may be expressed as $r = \rho^{-1}(a, 0) = \rho^{-1}(u'_1, 1) - \rho^{-1}(u'_2, 1)$, which is a difference of the two quadratic units $u_j = \rho^{-1}(u'_j, 1)$. Thus every even residue can be reached in $G_n$ by a path of length two from 0. As every odd residue is adjacent to an even residue, we may reach any vertex by a path of length at most three; then $\mathrm{diam}(G_n) = 3$.
- If $N = 4$ or $N$ is a multiple of 6, we have $u \in Q_N$ if and only if $u \equiv 1 \pmod{\bar{N}}$, where $\bar{N} = 4$ if $N = 4$, and $\bar{N} = 6$ otherwise. We may easily show that the only residues $r \in \mathbb{Z}_n$ which may be expressed as a difference of two quadratic units are those such that $r \equiv 0 \pmod{\bar{N}}$; and for any residue $a \equiv 0 \pmod{p_j}$, we have $S_M(a) = S_M(-a) = 0$ by Lemma 5. Therefore, no residue $r = \rho^{-1}(a, \pm 2) \in \mathbb{Z}_n$ can be reached by a path of length two from 0 in $G_n$. As any sum of the form $\pm u_1 \pm u_2 \pm u_3$ will be odd for $u_1, u_2, u_3 \in Q_n$, such residues $r$ are in fact at a distance at least four from zero. As $\mathrm{diam}(G_n) \leqslant 3 + \delta_3(n) = 4$, it follows that $\mathrm{diam}(G_n) = 4 = 3 + \delta_3(n)$ in this case.

In each case, the diameters agree with the formula in (10). □

## 3.5 Perfectness

A graph $G$ is *perfect* [10] if, for every induced subgraph $H \subseteq G$, the size $\omega(H)$ of the maximum clique in $H$ is equal to the chromatic number $\chi(H)$. This implies, in particular, that $G$ contains no *odd holes* (induced cycles of length $2k + 1$ for $k > 1$). Chudnovsky, Robertson, Seymour, and Thomas [11] characterized perfect graphs in terms of odd holes, proving a conjecture of Berge [12]:

**Strong Perfect Graph Theorem.** *A graph $G$ is perfect if and only if neither $G$ nor its complement $\bar{G}$ contain odd holes.*

**Lemma 11.** *For $n$ even or $n = p^m$ for $p \equiv 3 \pmod 4$ prime, $G_n$ is perfect.*

*Proof.* If $n$ is even, $G_n$ is bipartite, in which case $\omega(G_n) = \chi(G_n) = 2$. Otherwise, suppose that $n = p^m$ for a prime $p \equiv 3 \pmod 4$. Consider any path $x\ y\ z$ of length two in $G_n$ such that $z$ is non-adjacent to $x$. As every unit is either a quadratic residue or the negation of a quadratic residue modulo $p^m$, it follows that $x - z$ is not a unit. As $x \equiv z \pmod p$, we then have $x - t \equiv z - t \pmod p$ for any $t \in \mathbb{Z}_{p^m}$. The neighborhoods of $x$ and $z$ are then the same, so that for any $t$ adjacent to $z$, we obtain a cycle $x\ y\ z\ t\ x$ in $G_n$; thus $G_n$ does not contain induced cycles of length greater than four. As $\bar{G}_n$ consists of $p$ copies of the $p^{m-1}$-clique (with each clique consisting of some residue class modulo $p$), it also contains no odd holes; then $G_n$ is perfect. □

For any vertex colouring, the vertices of a given colour form an independent set by definition; if $\alpha(G)$ is the size of the largest independent set in $G$, we then have $\chi(G) \geqslant |V(G)|/\alpha(G)$. Thus, any self-complementary graph $G$ on $n$ vertices is perfect only if $\omega(G) \geqslant \sqrt{n}$. Maistrelli and Penman [13] use this to show that the Payley graphs of prime order are not perfect.[2] Noting that odd-order Paley graphs are also quadratic unitary Cayley graphs, we may extend this result as follows:

**Theorem 12.** *$G_n$ is perfect if and only if $n$ is even, or $n = p^m$ for $p \equiv 3 \pmod 4$ prime.*

*Proof.* Using Lemma 11, it suffices to show that $G_n$ is not perfect if $n$ is odd and is not a power of a prime $p \equiv 3 \pmod 4$. We consider the cases of $n$ divisible by an odd prime $p \equiv 1 \pmod 4$, and the case where $n$ is divisible by $p_1 p_2$ for distinct primes $p_1, p_2 \equiv 3 \pmod 4$. In either case, we may obtain a simpler graph $G_\nu$, for $\nu$ a factor of $n$, which has an odd hole:

- Suppose that $n$ has a prime factor which is equivalent to $1 \pmod 4$: if $n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$, we may suppose $p_1 \equiv 1 \pmod 4$ without loss of generality. We then take $\nu = p_1$. The graph $G_\nu$ is then self-complementary, as multiplication of any pair of adjacent vertices by a non-quadratic unit $r$ yields a non-adjacent pair, and vice-versa. However, we have $\omega(G_\nu) < \sqrt{\nu}$ by [13], so that $G_\nu$ is not perfect.

- Suppose instead that $n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$, for $p_1, p_2 \equiv 3 \pmod 4$: we then take $\nu = p_1 p_2$. For $r \in \mathbb{Z}_\nu^\times$ such that $r$ is a quadratic unit modulo $p_1$ but the negation of a quadratic residue modulo $p_2$, multiplication by $r$ maps adjacent pairs of vertices (whose difference is either a quadratic residue modulo both $p_1$ and $p_2$ or the negation of one modulo both residues) to non-adjacent pairs (where the status of the difference as a quadratic residue differ modulo $p_1$ and $p_2$). Therefore, $G_\nu$ is self-complementary.

  As two vertices $v, w \in V(G_\nu)$ are adjacent only if $v - w \not\equiv 0 \pmod{p_1}$ and $v - w \not\equiv 0 \pmod{p_2}$, the residues of two vertices in any clique modulo either $p_1$ and $p_2$ must differ. It then follows that $\omega(G_\nu) \leqslant \min\{p_1, p_2\} < \sqrt{\nu}$, so that $G_\nu$ is not perfect.

In both cases, $G_\nu$ contains an induced cycle $x'_1\, x'_2 \cdots x'_\ell\, x'_1$ for some odd $\ell \geqslant 5$ (again, as $G_\nu$ is self-complementary in both cases above). Let

$$\mu \;=\; \begin{cases} p_1^{m_1}, & \text{if } \nu = p_1, \\ p_1^{m_1} p_2^{m_2}, & \text{if } \nu = p_1 p_2 : \end{cases} \tag{13}$$

we may then obtain a similar odd hole in $G_\mu$ by identifying each $x'_j$ with a corresponding $x_j \in \{0, \ldots, \nu - 1\} \subseteq \mathbb{Z}_\mu$. Then $x_j - x_k \in Q_\mu$ if and only if $x'_j - x'_k \in Q_\nu$ for any $1 \leqslant j, k \leqslant \ell$, which implies that $x_1\, x_2 \cdots x_\ell\, x_1$ is a cycle without chords in $G_\mu$.

Let $N$ be the largest factor of $n$ which is coprime to $\mu$ (*i.e.* $N = n/\mu$), and let $\rho : \mathbb{Z}_n \longrightarrow \mathbb{Z}_\mu \oplus \mathbb{Z}_N$ be the natural isomorphism.

[2] This is in fact the simplest case of a more comprehensive theorem, which shows that the only perfect Paley graph is that on nine vertices.

- Suppose $\nu = p_1 \equiv 1 \pmod 4$. If $n$ is a multiple of 5, we may suppose that $p_1 = 5$ without loss of generality; then $N$ is coprime to 5. By Lemma 5, we then have $S_N(r) > 0$ for any $-r \in Q_N$: then $G_N$ contains a closed walk $0\ u\ r\ 0$ for some $u \in Q_N$. We may then construct a closed walk $y_1\, y_2 \cdots y_\ell\, y_1$ in $G_N$ by setting $y_1 = 0$, $y_2 = u$, $y_3 = r$, $y_4 = 0$, and concatenating this initial walk with $\frac{1}{2}(\ell - 3)$ copies of the walk $0\, u\, 0$. We may then construct a walk

$$C = (x_1, y_1)\ (x_2, y_2)\ \cdots\ (x_\ell, y_\ell)\ (x_1, y_1) \tag{14}$$

  in $G_\mu \otimes G_N$: because $x_1\, x_2 \cdots x_\ell\, x_1$ is an induced cycle, so is $C$.

- Otherwise, suppose $\mu = p_1^{m_1} p_2^{m_2}$. If $n$ is a multiple of 3, we may suppose that $p_1 = 3$ without loss of generality; then $N$ is coprime to 3. By Theorem 7, we then have $\ell > \mathrm{udiam}(\Gamma_N)$, in which case by Lemma 8 we may construct a closed walk $y_1\, y_2 \cdots y_\ell\, y_1$ in $G_N$ by setting $y_1 = 0$, and letting $y_{j+1} - y_j \in Q_N$ (or $y_{j+1} - y_j \in -Q_N$) whenever $x_{j+1} - x_j \in Q_\mu$ (respectively $y_{j+1} - y_j \in -Q_\mu$), and similarly for $y_1 - y_\ell$. Define the walk $C$ in $\mathbb{Z}_\mu \oplus \mathbb{Z}_N$ as given in (14): we then have $(x_{j+1}, y_{j+1}) - (x_j, y_j) \in \pm(Q_\mu \oplus Q_\nu)$ for each $j$, and similarly $(x_1, y_1) - (x_\ell, y_\ell) \in \pm(Q_\mu \oplus Q_N)$.

In either case, if we define vertices $v_j = \rho^{-1}(x_j, y_j) \in V(G_n)$, the walk $v_1\, v_2 \cdots v_\ell\, v_1$ is an induced cycle of odd length in $G_n$. Thus $G_n$ is not perfect, unless $n$ is even or a power of a prime $p \equiv 3 \pmod 4$. □

# 4 Decomposing symplectic operators mod $n$

Our final result is a bound on the complexity of decompositions of symplectic operastors modulo $n$, which follows from the bound on the diameter of $G_n$. We may define the *symplectic form* (modulo $n$) as the $2m \times 2m$ matrix

$$\sigma_{2m} \;=\; \begin{bmatrix} 0_m & -I_m \\ I_m & 0_m \end{bmatrix}; \tag{15}$$

the *symplectic group modulo* $n$ $\mathrm{Sp}_{2m}(\mathbb{Z}_n)$ is the set of $2m \times 2m$ linear operators $S$ (*symplectic operators*) with coefficients in $\mathbb{Z}_n$ such that $S^\top \sigma_{2m} S = \sigma_{2m}$.

**Convention.** For operators $S \in \mathrm{Sp}_{2m}(\mathbb{Z}_n)$ for a fixed $m$, we will adopt the convention of indexing the rows and columns by integers modulo $2m$, starting with 1. Thus, for a row $k \in \{m+1, \ldots, 2m\}$ in the "bottom" half of a matrix $S$, the row $k + m \in \{1, \ldots, m\}$ will be in the "top" half, and vice-versa.

Symplectic operators are clearly invertible operations, and therefore may be reduced to $I_{2m}$ by Gaussian elimination. We also consider a variant procedure, in which row-operations are constrained to themselves be symplectic. For the operator definitions below, actions of operators are defined via the action of left-multiplication on a square matrix over $\mathbb{Z}_n$.

**Definition IV.** For row-indices $j, k \in \{1, \ldots, 2m\}$, a *symplectic row operation acting on* $\mathrm{Sp}_{2m}(\mathbb{Z}_n)$ is one of the operators $M_j^{(\alpha)}$, $E_{j,k}$, $C_{j,k}$, or $C_{j,k}^{-1}$ defined as follows:

- For any $\alpha \in \mathbb{Z}_n^\times$, let $\mu_j^{(\alpha)} \in \mathrm{GL}_{2n}(\mathbb{Z}_n)$ be the linear operator which multiplies the $j^{\text{th}}$ row of its operand by $\alpha$. Then, we define $M_j^{(\alpha)} = \mu_j^{(\alpha)} \mu_{j+m}^{(\alpha^{-1})}$.
- Let $\varepsilon_{j,k} \in \mathrm{GL}_{2m}(\mathbb{Z}_n)$ be the linear operator which exchanges rows $j$ and $k$ of its operand. Then we define

$$E_{j,k} = \begin{cases} \varepsilon_{j,k}\, \mu_k^{(-1)}, & \text{if } j - k \equiv m \pmod{2m}; \\ \varepsilon_{j,k}\, \varepsilon_{j+m,k+m} & \text{otherwise,} \end{cases} \tag{16}$$

  for $\mu_j^{(-1)}$ as defined above.
- Let $\chi_{j,k} \in \mathrm{GL}_{2m}(\mathbb{Z}_n)$ be the linear operator which adds row $j$ of its operand to row $k$. Then we define

$$C_{j,k} = \begin{cases} \chi_{j,k}\,, & \text{if } j - k \equiv m \pmod{2m}; \\ \chi_{j,k}\, \chi_{k+m,j+m}^{-1}\,, & \text{if } 1 \leqslant j, k \leqslant m \text{ or } m+1 \leqslant j, k \leqslant 2m; \\ \chi_{j,k}\, \chi_{k+m,j+m}\,, & \text{otherwise.} \end{cases} \tag{17}$$

These operations are defined so as to be symplectic themselves; we wish to demonstrate an upper bound to the number of such symplectic row operations required to transform an arbitrary symplectic operator to the identity.

Hostens *et al.* [14] provide a decomposition of symplectic operators into $O(m^2 \log(n))$ symplectic row operations, in an application to the the decomposition of an important family of unitary operators for quantum computation (specifically, the Clifford group over qudits of dimension $n$). We refine this decomposition to obtain an upper bound to $O(m^2)$, giving an upper bound which is independent of the modulus $n$.

## 4.1 Reduction to greatest common divisors modulo $n$

We first describe the decomposition of [14] in detail. The main concept is to reduce $S \in \mathrm{Sp}_{2m}(\mathbb{Z}_n)$ to another operator $S'$ which acts trivially on, *e.g.*, the standard basis vectors $\hat{\mathbf{e}}_m, \hat{\mathbf{e}}_{2m}$. This reduces the problem to decomposing an operator $\tilde{S} \in \mathrm{Sp}_{2m-2}(\mathbb{Z}_n)$,

$$\tilde{S} = \begin{bmatrix} A'_{11} & A'_{12} \\ A'_{21} & A'_{22} \end{bmatrix} \qquad \text{for } S' = \left[\begin{array}{c|c|c|c} & 0 & & 0 \\ A'_{11} & \vdots & A'_{12} & \vdots \\ & 0 & & 0 \\ \hline 0 \cdots 0 & 1 & 0 \cdots 0 & 0 \\ \hline & 0 & & 0 \\ A'_{21} & \vdots & A'_{22} & \vdots \\ & 0 & & 0 \\ \hline 0 \cdots 0 & 0 & 0 \cdots 0 & 1 \end{array}\right]. \tag{18}$$

Embedding the matrix groups $\mathrm{Sp}_2(\mathbb{Z}_n) \subseteq \cdots \subseteq \mathrm{Sp}_{2m-2}(\mathbb{Z}_n) \subseteq \mathrm{Sp}_{2m}(\mathbb{Z}_n)$ in the manner described above, one may recursively apply this process to obtain a sequence of symplectic row operations which multiply to transform $S$ to $I_{2m}$. As the inverse of each symplectic row operation is also a symplectic row operation, this yields a decomposition of $S$.

The reduction from $S$ to $S'$ as above is performed by a hybrid of Gaussian elimination and Euclid's algorithm for computing greatest common divisors. We illustrate this on a $2m \times 2$ matrix $[\ \mathbf{v}\ \mathbf{w}\ ]$, for a pair of column vectors $\mathbf{v} = [\ v_1\ \ v_2\ \ \cdots\ \ v_{2m}\ ]^\top$ and $\mathbf{w} = [\ w_1\ \ w_2\ \ \cdots\ \ w_{2m}\ ]^\top$ subject to the constraint $\mathbf{w}^\top \sigma_{2m} \mathbf{v} = 1$. By performing suitable symplectic row-additions, we may simulate the Euclidean algorithm in the second column, for each pair of rows $(j,\, j+m)$ for $j \in \{1, \ldots, m\}$, to obtain

$$\left[\begin{array}{cc} v_1 & w_1 \\ v_2 & w_2 \\ \vdots & \vdots \\ v_m & w_m \\ \hline v_{m+1} & w_{m+1} \\ v_{m+2} & w_{m+2} \\ \vdots & \vdots \\ v_{2m} & w_{2m} \end{array}\right] \longmapsto \left[\begin{array}{cc} \tilde{v}_1 & 0 \\ \tilde{v}_2 & 0 \\ \vdots & \vdots \\ \tilde{v}_m & 0 \\ \hline \tilde{v}_{m+1} & \gcd(w_1, w_{m+1}, n) \\ \tilde{v}_{m+2} & \gcd(w_2, w_{m+2}, n) \\ \vdots & \vdots \\ \tilde{v}_{2m} & \gcd(w_m, w_{2m}, n) \end{array}\right] =: \left[\begin{array}{cc} \tilde{v}_1 & 0 \\ \tilde{v}_2 & 0 \\ \vdots & \vdots \\ \tilde{v}_m & 0 \\ \hline \tilde{v}_{m+1} & \gamma_1 \\ \tilde{v}_{m+2} & \gamma_2 \\ \vdots & \vdots \\ \tilde{v}_{2m} & \gamma_m \end{array}\right], \tag{19a}$$

computing "greatest common divisors" (modulo $n$) in the lower block in the second column, and using these to clear the upper block. We then perform further row-additions to compute further greatest common divisors in the second column, in pairs of rows $(j, j+1)$ for $j \in \{m+1, \ldots, 2m-1\}$, in to perform the following transformation of the the second column:

$$\left[\begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \\ \hline \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_m \end{array}\right] \longmapsto \left[\begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \\ \hline 0 \\ \gcd(\gamma_1, \gamma_2) \\ \vdots \\ \gamma_m \end{array}\right] \longmapsto \cdots \longmapsto \left[\begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \\ \hline 0 \\ 0 \\ \vdots \\ \gcd(\gamma_1, \gamma_2, \ldots, \gamma_{2m}) \end{array}\right]. \tag{19b}$$

Note that as $\mathbf{w}^\top \sigma_{2m} \mathbf{v} = 1$, there is an integer combination of the coefficients of $\mathbf{w}$ which is equivalent to 1 modulo $n$; then

$$\gcd(\gamma_1, \ldots, \gamma_m) \;=\; \gcd(w_1, \ldots, w_{2m}, n) \;=\; 1\,. \tag{20}$$

The above row-transformations then transform the two-column matrix $[\,\mathbf{v}\ \ \mathbf{w}\,]$ as follows:

$$\left[\begin{array}{cc} v_1 & w_1 \\ v_2 & w_2 \\ \vdots & \vdots \\ v_m & w_m \\ \hline v_{m+1} & w_{m+1} \\ v_{m+2} & w_{m+2} \\ \vdots & \vdots \\ v_{2m} & w_{2m} \end{array}\right] \mapsto \left[\begin{array}{cc} v'_1 & 0 \\ v'_2 & 0 \\ \vdots & \vdots \\ 1 & 0 \\ \hline v'_{m+1} & 0 \\ v'_{m+2} & 0 \\ \vdots & \vdots \\ v'_{2m} & 1 \end{array}\right] =: \left[\begin{array}{cc} \mathbf{v}' & \hat{\mathbf{e}}_{2m} \end{array}\right], \tag{21}$$

where $v'_m = 1$ follows from $\hat{\mathbf{e}}_{2m}^\top \sigma_{2m} \mathbf{v}' = \mathbf{w}^\top \sigma_{2m} \mathbf{v} = 1$. We may repeat the sequence of transformations to compute greatest common divisors in the first column, for each pair of rows $(j, j+m)$ for $j \in \{1, \ldots, m\}$, and subsequently in row-pairs $(j, j+1)$ in the upper block:

$$\left[\begin{array}{cc} v'_1 & 0 \\ v'_2 & 0 \\ \vdots & \vdots \\ 1 & 0 \\ \hline v'_{m+1} & 0 \\ v'_{m+2} & 0 \\ \vdots & \vdots \\ v'_{2m} & 1 \end{array}\right] \mapsto \left[\begin{array}{cc} \varphi_1 & 0 \\ \varphi_2 & 0 \\ \vdots & \vdots \\ 1 & 0 \\ \hline 0 & 0 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 1 \end{array}\right] \mapsto \left[\begin{array}{cc} 0 & 0 \\ \gcd(\varphi_1, \varphi_2) & 0 \\ \vdots & \vdots \\ 1 & 0 \\ \hline 0 & 0 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 1 \end{array}\right] \mapsto \left[\begin{array}{cc} 0 & 0 \\ 0 & 0 \\ \vdots & \vdots \\ 1 & 0 \\ \hline 0 & 0 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 1 \end{array}\right]. \tag{22}$$

The reduction of [14] applies this procedure for $\mathbf{v} = S\hat{\mathbf{e}}_m$, $\mathbf{w} = S\hat{\mathbf{e}}_{2m}$. Applying these transformations to $S$ yields a matrix $S'$ as illustrated in (18), as the other columns $S'\hat{\mathbf{e}}_k$ for $k \notin \{m, 2m\}$ must satisfy

$$\hat{\mathbf{e}}_k^\top S' \sigma_{2m} \hat{\mathbf{e}}_m \;=\; \hat{\mathbf{e}}_k S \sigma_{2m} S \hat{\mathbf{e}}_m \;=\; 0, \tag{23}$$

and similarly $\hat{\mathbf{e}}_k^\top S' \sigma_{2m} \hat{\mathbf{e}}_{2m} = 0$. The complexity of a single iteration of this reduction is $O(m \log(n))$, which arises from the cost of repeating Euclid's algorithm (expressed in fixed-width integer addition steps) $O(m)$ times to reduce the $m^{\text{th}}$ and $2m^{\text{th}}$ columns to $\hat{\mathbf{e}}_m$ and $\hat{\mathbf{e}}_{2m}$ respectively. Iterated $m$ times over all column-pairs $\hat{\mathbf{e}}_j, \hat{\mathbf{e}}_{j+m}$, we obtain the upper bound of $O(m^2 \log(n))$ reported by [14].

## 4.2 Improved upper bounds via the diameter of $G_n$

The complexity of the above decomposition may be reduced to $O(m^2)$, by substituting an explicit simulation of Euclid's algorithm via symplectic row transformations with a product of constant size. This is possible by using short paths in the graphs $G_n$ to reduce

the number of addition steps in order to obtain coefficients $\gamma_j$ and $\varphi_j$ (or coefficients equivalent to them, up to a multiplicative unit) using a constant number of row-operations.

The primary obstacle to reducing the complexity of a single iteration of the reduction of [14] is the computation of greatest common divisors in row-pairs $(j, j+m)$, arising from constraints on obtaining "derived" row-additions on these row-pairs. The iterated operator $C_{j,k}^{\alpha}$ (for $\alpha \in \{0, 1, \ldots, n-1\}$, which we identify with $\alpha \in \mathbb{Z}_n$) can be easily obtained in constant depth for $j \not\equiv k+m \pmod{2m}$ and $\alpha \in \mathbb{Z}_n^{\times}$, by the equality

$$C_{j,k}^{\alpha} \;=\; M_j^{(\alpha^{-1})}\, C_{j,k}\, M_j^{(\alpha)} \;, \tag{24a}$$

which one may verify by the action on standard basis vectors. However, $C_{j,j+m}^{\alpha}$ cannot be decomposed in this manner: the closest we may come is in the case where $\alpha = u^2$ for some $u \in \mathbb{Z}_n^{\times}$, in which case we have

$$C_{j,k}^{\alpha} \;=\; C_{j,k}^{u^2} \;=\; M_j^{(u^{-1})}\, C_{j,j+m}\, M_j^{(u)} \;. \tag{24b}$$

We may apply the result of Theorem 10 as follows:

**Lemma 13.** *For distinct row-indices $j, k \in \{1, \ldots, 2m\}$ and for any $\alpha \in \mathbb{Z}_n$, there exists a sequence of units $a_1, \ldots, a_\ell \in \mathbb{Z}_n^{\times}$ and signs $s_1, \ldots, s_\ell \in \{-1, +1\}$ for some $\ell \leqslant 12$, such that*

$$C_{j,k}^{\alpha} \;=\; M_j^{a_1^{-1}} C_{j,k}^{s_1} M_j^{a_2^{-1}a_1}\, C_{j,k}^{s_2} M_j^{a_3^{-1}a_2} \;\cdots\; M_j^{a_\ell^{-1}a_{\ell-1}} C_{j,k}^{s_\ell} M_j^{a_\ell} \;. \tag{25}$$

*Proof.* It suffices to note that as $\operatorname{diam}(G_n) \leqslant 12$, there exists such a sequence of signs and quadratic units $u_1, \ldots, u_\ell \in Q_n$ such that $\alpha = s_1 u_1 + s_2 u_2 + \cdots + s_\ell u_\ell$. We may then take either $a_j = u_j$ (in the case that $k \neq j+m$) or a unit $a_j$ such that $u_j = a_j^2$ (in the case that $k = j+m$), and apply the decompositions of (24) to obtain the desired decomposition.[3] □

We may apply this to reduce the complexity of decomposing symplectic operators as follows. We use the following additional Lemma, whose proof is deferred to the appendix:

**Lemma 14.** *Let $\gamma = \gcd(x, y, n)$: then there exist $a, b, c \in \mathbb{Z}$ such that $ax + by + cn = \gamma$ and where both $a$ and $b$ are relatively prime to $n$.*

For a vector $\mathbf{x} = [\; x_1 \quad x_2 \quad \cdots \quad x_{2m} \;]^{\top}$, let $\gamma_j = \gcd(x_j, x_{j+m}, n)$ for each $j \in \{1, \ldots, m\}$. Let $a_j$ be coefficients such that $a_{j+m} x_{j+m} + a_j x_j \equiv \gamma_j \pmod{n}$ as guaranteed

[3] For $k \neq j+m$, we may in fact obtain the further bound of $\ell \leqslant 3$, as the diameter of the unitary Cayley graph $X_n = \operatorname{Cay}(\mathbb{Z}_n, \mathbb{Z}_n^{\times})$ is at most three [4].

by Lemma 14, and define $r_j = a_{j+m}^{-1} a_j$: we then have

$$C_{1,m+1}^{r_1} \cdots C_{m,2m}^{r_m} \mathbf{x} = \left[\begin{array}{c} x_1 \\ x_2 \\ \vdots \\ x_m \\ \hline x_{m+1} + a_{m+1}^{-1} a_1 x_1 \\ x_{m+2} + a_{m+2}^{-1} a_2 x_2 \\ \vdots \\ x_{2m} + a_{2m}^{-1} a_m x_m \end{array}\right] = \left[\begin{array}{c} x_1 \\ x_2 \\ \vdots \\ x_m \\ \hline a_{m+1}^{-1}\gamma_1 \\ a_{m+2}^{-1}\gamma_2 \\ \vdots \\ a_{2m}^{-1}\gamma_m \end{array}\right] =: \left[\begin{array}{c} x_1 \\ x_2 \\ \vdots \\ x_m \\ \hline \tilde{\gamma}_1 \\ \tilde{\gamma}_2 \\ \vdots \\ \tilde{\gamma}_m \end{array}\right]. \tag{26}$$

Each coefficient $\tilde{\gamma}_j$ generates the same additive subgroup as $\gamma_j$ modulo $n$; if $d_1, \ldots, d_m$ are coefficients such that $x_j = d_m a_{j+m}^{-1} \gamma_j = d_m \tilde{\gamma}_j$, we then have

$$C_{m+1,1}^{-d_1} \cdots C_{2m,m}^{-d_m} \left[\begin{array}{cccccc} x_1 & \cdots & x_m & \tilde{\gamma}_1 & \cdots & \tilde{\gamma}_m \end{array}\right]^\top = \left[\begin{array}{cccccc} 0 & \cdots & 0 & \tilde{\gamma}_1 & \cdots & \tilde{\gamma}_m \end{array}\right]^\top. \tag{27}$$

The above performs the reduction of (19a), up to multiplicative units, in $O(m)$ symplectic row operations. We may similarly emulate the reductions of (19b) and (22) in $O(m)$ symplectic row operations, using Lemma 14 to reduce the computation of greatest common divisors (up to multiplicative unit factors) to performing powers of the operators $C_{j,k}$.

To summarize, using the bound on the diameter of the quadratic unitary graph $G_n$, we may refine the decomposition of symplectic operators in [14] by substituting an explicit simulation of Euclid's algorithm by a constant-size sequence of symplectic operations. This substitution provides an upper bound of $O(m^2)$ for a decomposition of an operator $S \in \mathrm{Sp}_{2m}(\mathbb{Z}_n)$, a bound independent of the modulus $n$.

# 5 Remarks and open problems

It should be noted that quadratic unitary graphs, while easy to describe, are closely tied to unsolved problems in computational complexity theory. In particular, testing adjacency in a graph $G_n$ is precisely the quadratic residuacity problem, which has no known efficient algorithms and is considered unlikely to be efficiently solvable (see *e.g.* Chapter 3 of [15]).[4] Because of this, an efficient algorithm (deterministic or randomized) for discovering the shortest path between two vertices in $G_n$ should be considered unlikely. We may then ask whether there are efficient algorithms for discovering "short" paths (having length bounded by a fixed constant) between vertices in $G_n$.

[4]It should be noted that because quadratic residuacity can be reduced to integer factoring (by exploiting the Chinese Remainder theorem), and because factoring is solvable in a polynomial number of operations with bounded error with a *quantum* computer [16], testing adjacency in $G_n$ is also tractible for a quantum computer.

In Section 3.5, we provided a non-constructive proof that odd holes arise in quadratic unitary graphs $G_n$ which are odd but not a power of a prime $p \equiv 3 \pmod 4$. Numerical investigation suggests that, in particular, *five-holes* (odd holes of size five) are very common in those $G_n$ which are not perfect graphs, even when restricting to five-holes involving the arc $0 \to 1$. An explicit construction of five-holes in $G_n$, for all $n$ for which they exist, is likely to require insights into the structure of quadratic residues beyond the results used in this article.

As we noted in the introduction and in Section 3.5, the graphs $G_n$ for $n \equiv 1 \pmod 4$ prime are also Paley graphs. Shparlinski [17] shows that prime-order Paley graphs these graphs have high *energy* (*i.e.* the operator 1-norm of the adjacency matrix), coming to within a factor of $(1 - \frac{1}{n})$ of the upper bound $\mathcal{E}_{\max}(n) = \frac{1}{2}n(\sqrt{n} + 1)$ shown in [18] for graphs on $n$ vertices. We may ask to what extent this and other properties of circulant Paley graphs generalize for quadratic unitary graphs.

# References


[1] P. Erdős, A. B. Evans. *Representations of graphs and orthogonal Latin square graphs.* J. Graph Theory **13** (pp. 593–595), 1989.

[2] I. Dejter, R. E. Giudici. *On unitary Cayley graphs.* J. Combin. Math. Combin. Comput. **18** (pp. 121–124), 1995.

[3] P. Berrizbeitia, R. E. Giudici. *On cycles in the sequence of unitary Cayley graphs.* Discrete Math. **282** (pp. 1–3), 2004.

[4] W. Klotz, T. Sander. *Some Properties of Unitary Cayley Graphs.* Elec. J. Combinatorics **14**, 2007.

[5] H. N. Ramaswamy, C. R. Veena. *On the Energy of Unitary Cayley Graphs.* Elec. J. Combinatorics **16**, 2009.

[6] P. M. Weichsel. *The Kronecker Product of Graphs.* Proc. of the AMS **13** (pp. 47–52), 1962.

[7] C. F. Gauss. *Disquisitiones Arithmeticæ— English Edition.* Springer-Verlag, New York-Heidelberg, 1986.

[8] S. Klavzar, S. Severini. *Tensor 2-sums and entanglement.* Preprint [`arXiv:0909.1039`], 2009.

[9] N. S. Aladov. *On the distribution of quadratic residues and nonresidues of a prime number p in the sequence* $1, 2, \ldots, p-1$. Mat. Sbornik **18** (pp. 61–75), 1896. (Russian)

[10] J. L. R. Alfonsin, B. A. Reed. *Perfect Graphs.* John Wiley & Sons, New York-Chichester-Brisbane, 2001.

[11] M. Chudnovsky, N. Robertson, P. Seymour, R. Thomas. *The strong perfect graph theorem.* Annals of Math. **164**, (pp. 51–229), 2002.

[12] C. Berge. *Färbung von Graphen, deren sämtliche bzw. deren ungerade Kreise starr sind.* Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe **10** (pp. 114–115), 1961.

[13] E. Maistrelli, D. B. Penman. *Some colouring problems for Paley graphs.* J. Discrete Math. **306** (pp. 99–106), 2006.

[14] E. Hostens, J. Dehaene, and B. De Moor. *Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic.* Phys. Rev. A **71** (042315), 2005. [arXiv:quant-ph/0408190]

[15] A. J. Menezes, S. A. Vanstone, P. C. Van Oorschot. *Handbook of Applied Cryptography.* CRC Press, Inc., Boca Raton, 1996.

[16] P. W. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* SIAM J. Sci. Statist. Comput. **26** (pp. 1484–1509), 1997.

[17] I. Shparlinski. *On the energy of some circulant graphs.* Linear Algebra Appl. **414** (pp. 371–382), 2006.

[18] J. H. Koolen, V. Moulton. *Maximal energy graphs.* Adv. Appl. Math. **26** (pp. 47–52), 2001.

# A The existence of special Bézout coefficients

For a sequence of integers $x_1, x_2, \ldots, x_k$, *Bézout coefficients* are a corresponding sequence of integer coefficients $a_1, a_2, \ldots, a_k$ such that $\gcd(x_1, \ldots, x_k) = \sum a_j x_j$; the existence of such a sequence of coefficients $a_1, \ldots, a_k$ is implied by the "simple" Euclidean algorithm.

Consider the greatest common divisior of a sequence $x_1, \ldots, x_k$ together with another integer $n$: this is equivalent to computing $\gamma = \gcd(x_1, \ldots, x_k)$ modulo $n$ via Euclid's algorithm. We may compute greatest common divisors modulo $n$ recursively, by computing $\gamma_2 = \gcd(x_1, x_2)$ modulo $n$, then $\gamma_3 = \gcd(\gcd(x_1, x_2), x_3)$ modulo $n$, and so forth. However, for each intermediate stage $1 < j < k$, it is not necessary to obtain $\gamma_j$ itself, but instead a similar residue $\tilde{\gamma}_j$ which generates the same subgroup modulo $n$; by definition, the set of integer combinations modulo $n$ of such an integer $\tilde{\gamma}_j$ is the same as the set of integer combinations of $\gamma_j$, so that $\gcd(a, \tilde{\gamma}_j) \equiv \gcd(a, \gamma_j) \pmod{n}$ for any $a \in \mathbb{Z}$.

The simplest application of this observation is that in $\mathbb{Z}_n$, any integer $x$ may serve as a substitute for its own greatest common divisor with $n$:

**Lemma 15.** *Let $\gamma = \gcd(x, n)$ for $x, n \in \mathbb{Z}$: then there exist $a, b \in \mathbb{Z}$ such that $ax + bn = \gamma$ and where $a$ is relatively prime to $n$.*

*Proof.* Consider arbitrary $a, b \in \mathbb{Z}$ such that $ax + bn = \gamma$. Let $\alpha = \gcd(a, \gamma)$: then $\alpha$ divides $a$, $x$, and $n$. We have $\frac{a}{\alpha}x = (\frac{\gamma}{\alpha} - b\frac{D}{\alpha}) \in \frac{\gamma}{\alpha}\mathbb{Z}$. By construction, $\frac{a}{\alpha}$ is an integer relatively prime to $\frac{\gamma}{\alpha}$: thus, $x$ is a multiple of $\frac{\gamma}{\alpha}$. Let $m = \frac{\alpha x}{\gamma}$: then $\frac{m}{\alpha} = \frac{x}{\gamma} \in \mathbb{Z}$, and furthermore is relatively prime to $n$. Then, if we let $\bar{a} \in \mathbb{Z}$ be such that $\frac{\bar{a}m}{\alpha} \equiv 1 \pmod{n}$, we have $\bar{a}x \equiv \gamma \pmod{n}$ as required. □

We generalize the above lemma as follows. In order to compute a suitable integer $\tilde{\gamma}_j$ which generates the same additive group (modulo $n$) as $\gamma_j = \gcd(\tilde{\gamma}_{j-1}, x_j)$ for each $j$, we may compute Bézout coefficients $a, b, c$ such that

$$ax_j + b\tilde{\gamma}_{j-1} + cn = \gamma_j. \tag{28}$$

If we may find such a set of coefficients that $a$ is coprime to $n$, we then have

$$x_j \; + \; \tilde{a}b\tilde{\gamma}_{j-1} \; \equiv \; \tilde{a}\gamma_j \pmod{n}\,, \tag{29}$$

where $a\tilde{a} \equiv 1 \pmod{n}$, in which case we may let $\tilde{\gamma}_j = \tilde{a}\gamma_j$. That is, if such $a \in \mathbb{Z}_n^\times$ exists, we may compute $\tilde{\gamma}_j$ as the sum of $x_j$ with some multiple of $\tilde{\gamma}_{j-1}$, which can be computed using a single addition operation and a single scalar multiplication. We show that such Bézout coefficients may always be found by proving Lemma 14 (page 21):

**Lemma 16.** *Let $\gamma = \gcd(x, y, n)$: then there exist $a, b, c \in \mathbb{Z}$ such that $ax + by + cn = \gamma$ and where both $a$ and $b$ are relatively prime to $n$.*

*Proof.* Let $x' = \gcd(x, n)$ and $y' = \gcd(y, n)$: by Lemma 15, we then have $x \equiv u_x x' \pmod{n}$ and $y \equiv u_y y' \pmod{n}$ for multiplicative units $u_x, u_y \in \mathbb{Z}_n^\times$, and $\gamma = \gcd(x', y')$. Define

$$\bar{x} \; = \; \frac{x'}{\gamma}\,, \qquad\qquad \bar{y} \; = \; \frac{y'}{\gamma}\,; \tag{30}$$

these are both divisors of $n$, and form a relatively prime pair. We may then partition the prime factors of $n$ into those which divide $\bar{x}$, those which divide $\bar{y}$, and those which divide neither. Let $N_x$ be the largest factor of $\bar{n}$ whose prime factors divide $\bar{x}$, $N_y$ be the largest factor of $\bar{n}$ whose prime factors divide $\bar{y}$, and $N_n = n/N_xN_y$: then $N_x$ and $N_y$ are coprime, so that $N_n$ is also an integer and relatively prime both to $N_x$ and $N_y$. We then have $n = N_xN_yN_n$.

As $\bar{x}$ and $\bar{y}$ are coprime, there exist integers $a, b \in \mathbb{Z}$ such that $a\bar{x} + b\bar{y} = 1$. Note that $a$ is coprime to $\bar{y}$, from which it follows that $a$ is coprime to $N_y$ as well, as $N_y$ and $\bar{y}$ have the same prime factors; similarly, $b$ is coprime to $N_x$. Let

$$h \; = \; \begin{cases} 0\,, & \text{if } \gcd(a, N_xN_d) = \gcd(b, N_yN_n) = 1; \\ N_y\,, & \text{if } \gcd(a, N_xN_d) > 1, \text{ but } \gcd(b, N_yN_n) = 1; \\ N_x\,, & \text{if } \gcd(a, N_xN_d) = 1, \text{ but } \gcd(b, N_yN_n) > 1; \\ 1\,, & \text{otherwise;} \end{cases} \tag{31}$$

and let $\alpha = a + h\bar{y}$ and $\beta = b - h\bar{x}$. If $a$ has prime factors in common with $N_x N_n$, then $\alpha$ does not, by the fact that both $\bar{y}$ and $\bar{y}N_y$ are relatively prime to $N_x N_n$ ; otherwise, $\alpha$ is coprime to $N_x N_n$ anyway by the coprimality of $a$ to $N_x N_n$. In either case, we also have $\alpha$ coprime to $N_y$, by the coprimality of $a$ and $\bar{y}$. Thus, $\alpha$ is relatively prime to $n = N_x N_y N_n$; and similarly, $\beta$ is coprime to $n$. We may then observe that

$$\alpha\bar{x} + \beta\bar{y} \;=\; (a + h\bar{y})\bar{x} + (b - h\bar{x})\bar{y} \;=\; a\bar{x} + b\bar{y} \;=\; 1\,, \tag{32}$$

from which it follows that $\alpha x' + \beta y' = \gamma$. Let $\bar{a}, \bar{b} \in \mathbb{Z}$ be such that $u_x \bar{a} \equiv \alpha \pmod{n}$ and $u_y \bar{b} \equiv \beta \pmod{n}$ : then, we have

$$\bar{a}x + \bar{b}y \;\equiv\; \alpha x' + \beta y' \;=\; \gamma \pmod{n}\,: \tag{33}$$

as $\alpha$, $u_x$, $\beta$, and $u_y$ are all coprime to $n$, both $\bar{a}$ and $\bar{b}$ are also coprime to $n$. □

# Corrigendum – submitted Jul 7, 2010

There is an unfortunate error in the proof of Theorem 12, in the case that n is divisible by two distinct primes $p_1, p_2 \equiv 3 \pmod 4$. It is easy to show that the graph $G_{p_1 p_2}$ is in fact not self-complementary. Therefore, for that particular case, the given approach would neither prove that $G_{p_1 p_2}$ is imperfect, nor that it has an odd hole if it is.

Fortunately, one may still prove the existence of odd holes for such graphs $G_{p_1 p_2}$. Better still, for three separate cases, one may explicitly construct odd holes of size five (or "five holes"). In what follows, we represent vertices by ordered pairs of residues modulo $p_1$ and $p_2$:

- In the case that 2 is not a quadratic residue modulo either $p_1$ or $p_2$, we let $p_1 < p_2$, which implies $p_2 = 11$ or $p_2 > 17$. There then exist consecutive triples of quadratic residues modulo $p_2$. If we let $q, q+1, q+2$ be a minimal such triple, one may show that the five vertices

$$a = (0,0); \qquad b = (1,1); \qquad c = (2, q+1); \qquad d = (0,2); \qquad e = (2, -q) \tag{34}$$

  induce a five-hole in $G_{p_1 p_2}$.

- In the case that 2 is a quadratic residue modulo exactly one of $p_1$ or $p_2$ (say the latter), we may show that the five vertices

$$a = (0,0); \qquad b = (1,1); \qquad c = (2,2); \qquad d = (0,3); \qquad e = (1,4) \tag{35}$$

  induce a five-hole in $G_{p_1 p_2}$.

- In the case that 2 is a quadratic residue modulo both $p_1$ and $p_2$, there will be pairs of consecutive quadratic residues modulo each of these primes. We let $q-1, q$ be the minimal such residues modulo $p_1$, and $q'-1, q'$ be the minimal such residues modulo $p_2$. It follows that $q'$ differs from $-1$, so that $-q'-1$ is a quadratic residue. We may then show that the five vertices

$$a = (0,0); \qquad b = (1,1); \qquad c = (q, -q') \qquad d = (0,1) \qquad e = (1, q') \tag{36}$$

  induce a five-hole in $G_{p_1 p_2}$.

Having explicitly constructed an odd hole in $G_{p_1 p_2}$, the rest of the proof carries forward verbatim. These "five-holes" partially solve an open problem in the original article; it would be interesting to obtain a classification of all five-holes in the imperfect graphs $G_n$, both in this case and in the case of $n$ divisible by a prime $p \equiv 1 \pmod 4$.

A new version of this article which incorporates these corrections is also available at [ `www.arxiv.org/abs/1002.0713` ] (v2 or higher).