Journal of Pure and Applied Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Cyclotomic graphs and perfect codes

Sanming Zhou

School of Mathematics and Statistics, The University of Melbourne, Parkville, VIC 3010, Australia

ARTICLE INFO

Article history:
Received 24 November 2015
Received in revised form 4 May 2018
Available online xxxx
Communicated by I.M. Duursma

MSC:
05C25; 68M10; 94A99

ABSTRACT

We study two families of cyclotomic graphs and perfect codes in them. They are Cayley graphs on the additive group of $\mathbb{Z}[\zeta_m]/A$, with connection sets $\{\pm(\zeta_m^i + A) : 0 \le i \le m-1\}$ and $\{\pm(\zeta_m^i + A) : 0 \le i \le \phi(m)-1\}$, respectively, where ζ_m $(m \ge 2)$ is an mth primitive root of unity, A a nonzero ideal of $\mathbb{Z}[\zeta_m]$, and ϕ Euler's totient function. We call them the mth cyclotomic graph and the second kind mth cyclotomic graph, and denote them by $G_m(A)$ and $G_m^*(A)$, respectively. We give a necessary and sufficient condition for D/A to be a perfect t-code in $G_m^*(A)$ and a necessary condition for D/A to be such a code in $G_m(A)$, where $t \ge 1$ is an integer and D an ideal of $\mathbb{Z}[\zeta_m]$ containing A. In the case when $m = 3, 4$, $G_m((\alpha))$ is known as an Eisenstein–Jacobi and Gaussian networks, respectively, and we obtain necessary conditions for $(\beta)/(\alpha)$ to be a perfect t-code in $G_m((\alpha))$, where $0 \ne \alpha, \beta \in \mathbb{Z}[\zeta_m]$ with β dividing α. In the literature such conditions are known to be sufficient when $m = 4$ and $m = 3$ under an additional condition. We give a classification of all first kind Frobenius circulants of valency $2p$ and prove that they are all pth cyclotomic graphs, where p is an odd prime. Such graphs belong to a large family of Cayley graphs that are efficient for routing and gossiping.

1. Introduction

Perfect codes have been important objects of study ever since the dawn of coding theory in the late 1940s, and after more than six decades they still receive much attention today. Hamming and Golay codes are well known examples of perfect codes, and their importance to information theory has been widely recognised. So far a large number of beautiful results on perfect codes have been produced, as seen in the survey papers [14,37]. As generalizations of perfect codes in the classical setting, in [3] Biggs initiated the study of perfect codes in distance-transitive graphs, namely those graphs whose automorphism groups are transitive on the set of ordered pairs of vertices at distance i, for every i from 0 to the diameter of the graph. In the same paper he generalized the celebrated Lloyd's Theorem in the classical setting to distance-transitive graphs. (Lloyd's Theorem asserts that if a perfect e-code of length n exists, then the zeros of a certain polynomial of degree e must be distinct integers among $1, 2, \ldots, n$.) Distance-transitive graphs are distance-regular graphs,

E-mail addresses: smzhou@ms.unimelb.edu.au, sanming@unimelb.edu.au.

https://doi.org/10.1016/j.jpaa.2018.05.007
0022-4049/

which in turn can be viewed as association schemes. In [5] Delsarte pioneered the study of perfect codes in association schemes. Since then a great deal of work has been done in this research direction (see e.g. [1,5,9]).

The study of perfect codes in general graphs began with [21]. A *code* in a graph $X = (V, E)$ is a non-empty subset of V. Given an integer $t \geq 1$, the *ball* with radius t and centre $v \in V$ is defined as $B_t(v, X) := \{u \in V : d(v, u) \leq t\}$, where $d(v, u)$ is the distance in X between v and u. A code $C \subseteq V$ is called a *perfect t-error-correcting code* or a *perfect t-code* in X if the balls $B_t(v, X)$ with radius t and centres $v \in C$ form a partition of V. In graph theory, $B_t(v, X)$ is called the *t-neighbourhood* of v in X, each vertex in $B_t(v, X)$ is said to be *t-dominated* by v, a perfect t-code in X is called a *perfect t-dominating set* of X, and a perfect 1-code in X is called an *efficient dominating set* or *independent perfect dominating set* (see e.g. [4,22,28,29]). A q-ary perfect t-code of length n in the classical setting is simply a perfect t-code in the corresponding Hamming graph $H(n, q)$.

Since $H(n, q)$ is a Cayley graph on $\mathbb{Z}_q^n$, perfect codes in Cayley graphs on finite groups can be thought as another avenue of generalizing perfect codes in the classical setting. Perfect codes in Cayley graphs are also closely related to factorizations and tilings of groups [17]. So far several results on perfect codes in Cayley graphs have been produced, but the area is still wide open. In [22] it was proved that a 'normal subset' of a group G is a perfect 1-code in a Cayley graph on G if and only if there exists a covering from the Cayley graph to a complete graph such that C is a fibre of the corresponding covering projection. (In [22] a subset C of G is called normal if $gC = Cg$ for any $g \in G$; this is equivalent to saying that C is closed under conjugation.) In [8] perfect 1-codes in a Cayley graph with connection set closed under conjugation were studied by way of equitable partitions, yielding a nonexistence result in terms of irreducible characters of the underlying group. In [17] several results about when a normal subgroup of a finite group is a perfect 1-code in some Cayley graph of the group were obtained.

In [32] it was proved that there is no perfect 1-code in any Cayley graph on $\mathrm{SL}(2, 2^f)$, $f > 1$ with respect to any connection set closed under conjugation. In [4] a methodology for constructing E-chains of Cayley graphs was given and was used to construct infinite families of E-chains of Cayley graphs on symmetric groups, where an *E-chain* is a countable family of nested graphs each containing a perfect 1-code. Perfect 1-codes in circulants were studied in [6,12,28,29], and those in directed products of cycles were completely characterized in [39]. In [24] sufficient conditions for Gaussian and Eisenstein–Jacobi graphs to contain perfect codes were given. Quotients of Gaussian graphs and their applications to constructing perfect codes were further discussed in [23]. In [25] a certain Cayley graph defined on the integer quaternions right-modulo a fixed nonzero element was introduced and perfect 1-codes in it were constructed.

In general, it is challenging to construct perfect codes in Cayley graphs – many Cayley graphs do not contain any perfect code at all. Inspired by [24] and our own work [36,40] on Frobenius graphs, in this paper we study the following two families of Cayley graphs and perfect codes in them. Let ζ_m ($m \geq 2$) be an mth primitive root of unity, say $\zeta_m = e^{2\pi i/m}$, and A a nonzero ideal of the ring $\mathbb{Z}[\zeta_m]$ of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_m)$. We define the *mth cyclotomic graph* with respect to A, denoted by $G_m(A)$, to be the Cayley graph on the additive group of the quotient ring $\mathbb{Z}[\zeta_m]/A$ with respect to the connection set $\{\pm(\zeta_m^i + A) : 0 \leq i \leq m-1\}$. We define the *second kind mth cyclotomic graph* with respect to A, denoted by $G_m^*(A)$, to be the Cayley graph on the same group with respect to the connection set $\{\pm(\zeta_m^i + A) : 0 \leq i \leq \phi(m)-1\}$, where ϕ is Euler's function. In the case when $m = 3, 4$, $G_3((\alpha))$ and $G_4((\alpha))$ are precisely the Eisenstein–Jacobi and Gaussian networks [13,24,26], respectively, where (α) is the principal ideal generated by $0 \neq \alpha \in \mathbb{Z}[\zeta_m]$. These two special families of cyclotomic graphs are closely related to two families of Frobenius circulants as shown in [41, Lemma 5] and [36, Theorem 5].

We prove that the distance in $G_m^*(A)$ between two vertices is the Mannheim distance [10,18] (Lemma 4.1). Based on this observation we give a necessary and sufficient condition (Lemma 4.2) for a subring D/A of $\mathbb{Z}[\zeta_m]/A$ to be a perfect t-code in $G_m^*(A)$ (that is, a perfect t-code on $\mathbb{Z}[\zeta_m]/A$ with respect to the Mannheim distance), where $t \geq 1$ and D is an ideal of $\mathbb{Z}[\zeta_m]$ containing A. We also give a necessary condition for D/A

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

to be a perfect t-code in $G_m(A)$ (Lemma 4.2). Applying this result to the case $m = 4$, we show that the sufficient condition given in [26, Theorems 18] for $(\beta)/(\alpha)$ to be a perfect t-code in the Gaussian network $G_4((\alpha))$ is also necessary (Theorem 4.5), where α and β are nonzero elements of $\mathbb{Z}[i]$ with β dividing α. We also give a necessary condition for $(\beta)/(\alpha)$ to be a perfect t-code in the Eisenstein–Jacobi network $G_3((\alpha))$ (Theorem 4.7), where α and β are nonzero elements of $\mathbb{Z}[\rho]$ (where $\rho = (1 + \sqrt{-3})/2$) with β dividing α. It was proved in [24, Theorem 24] that this necessary condition is sufficient in the case when $\alpha = a + b\rho$ with $\gcd(a, b) = 1$. We show that the condition $\gcd(a, b) = 1$ can be removed. Therefore, in the case when $m = 3, 4$, all perfect codes in $G_m((\alpha))$ of the form $(\beta)/(\alpha)$ are known explicitly. An example can be found at the end of the paper.

As mentioned above, one of the motivations for our work is the study of Frobenius graphs in the context of communication network design. Due to the work in [11,31,40] it is known that first kind Frobenius graphs are 'perfect' as far as routing and gossiping are concerned, in the sense that they achieve the smallest possible edge-forwarding and arc-forwarding indices [16,40] and the smallest possible gossiping time [40] under the store-and-forward, all-port and full-duplex model. (An *arc* in a graph is an ordered pair of adjacent vertices.) These features together with the importance of circulants as communication networks [2] make it desirable to classify first kind Frobenius circulants. This has been achieved in [33] and [36] in the case of valency 4 and 6, respectively. (See also [34,35,41] for related results.) In this paper we classify first kind Frobenius circulants of valency $2p$ for any odd prime p (Theorem 5.3), and prove that all of them are pth cyclotomic graphs (Theorem 5.5). Before establishing this connection we prove a few basic properties of cyclotomic graphs (Theorem 3.2). In particular, we prove that $G_m(A)$ is arc-transitive and rotational, and thus can be embedded on a closed orientable surface as a balanced regular Cayley map.

Many problems arise from our study in this paper. One of them is concerned with constructing more perfect codes in cyclotomic graphs, possibly with the help of Lemma 4.2 and Corollary 4.3. See Problem 5.7 in the special case where p is an odd prime such that $\mathbb{Z}[\zeta_p]$ is a principal ideal domain.

2. Notation and definitions

We follow [7] and [19,38], respectively, for terminology and notation in group theory and number theory. If G is a group acting on a set Ω and $\alpha \in \Omega$, the *stabilizer* of α in G is the subgroup $G_\alpha := \{g \in G : \alpha^g = \alpha\}$ of G and the G-*orbit* containing α is $\alpha^G := \{\alpha^g : g \in G\}$. If H and K are groups such that H acts on K as a group, the *semidirect product* $K \rtimes H$ is the group defined on the set $K \times H$ with operation given by $(x, u)(y, v) := (xy^{u^{-1}}, uv)$ for $(x, u), (y, v) \in K \times H$.

Given a group G and a subset S of G such that $1_G \notin S = S^{-1} := \{s^{-1} : s \in S\}$ (where 1_G is the identity element of G), the *Cayley graph* on G with respect to S, $\mathrm{Cay}(G, S)$, is defined to have vertex set G such that $x, y \in G$ are adjacent if and only if $xy^{-1} \in S$. A *complete rotation* [15] of $\mathrm{Cay}(G, S)$ is an automorphism of G which fixes S setwise and induces a cyclic permutation on S; $\mathrm{Cay}(G, S)$ is *rotational* if it admits a complete rotation. A Cayley graph on a cyclic group is called a *circulant*. More explicitly, for a subset S of the additive group of ring $\mathbb{Z}_n$ such that $[0] \notin S = -S := \{-s : s \in S\}$, $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a circulant of order n and valency $|S|$.

A transitive group G on Ω is called a *Frobenius group* [7] if it is not regular but only the identity element can fix two points of Ω. It is well known (see e.g. [7, Section 3.4]) that a finite Frobenius group G has a nilpotent normal subgroup K, called the *Frobenius kernel* of G, which is regular on Ω. Hence $G = K \rtimes H$, where H is the stabilizer of a point of Ω. Since K is regular on Ω, we may identify Ω with K in such a way that K acts on itself by right multiplication, and we choose H to be the stabilizer of 1_K so that H acts on K by conjugation. Thus an H-orbit on K is of the form $x^H := \{h^{-1}xh : h \in H\}$, where $x \in K$. A *first kind* G-*Frobenius graph* [11,40] is a Cayley graph $X = \mathrm{Cay}(K, S)$ on K, where $S = a^H$ for some $a \in K$ satisfying $\langle a^H \rangle = K$, with $|H|$ even or a an involution. By abusing terminology we say that X is a first kind Frobenius graph with *kernel* K.

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

All graphs in the paper are finite and undirected. A graph X is *k-valent* if all its vertices have valency k; in this case $k = \mathrm{val}(X)$ is called the valency of X. A graph X is *G-vertex-transitive* (*G-edge-transitive*, *G-arc-transitive*, respectively) if G is a subgroup of the automorphism group of X that is transitive on the set of vertices (edges, arcs, respectively) of X.

3. Cyclotomic graphs

In this section we introduce cyclotomic graphs and prove a few basic properties of them.

It is well known (see e.g. [38, Theorem 2.6]) that the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m] := \{a_0 + a_1\zeta_m + \ldots + a_{m-1}\zeta_m^{m-1} : a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}\}$. It is also known (see e.g. [38, Theorem 2.5]) that $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ with $1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}$ a basis for $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$.

Definition 3.1. Let $m \geq 2$ be an integer and $A \neq \{0\}$ an ideal of $\mathbb{Z}[\zeta_m]$. Define

$$G_m(A) := \mathrm{Cay}(\mathbb{Z}[\zeta_m]/A, E_m/A)$$

to be the Cayley graph on the additive group of $\mathbb{Z}[\zeta_m]/A$ with respect to

$$E_m/A := \{\pm(\zeta_m^i + A) : 0 \leq i \leq m-1\}. \tag{1}$$

Define

$$G_m^*(A) := \mathrm{Cay}(\mathbb{Z}[\zeta_m]/A, E_m^*/A)$$

to be the Cayley graph on the additive group of $\mathbb{Z}[\zeta_m]/A$ with respect to

$$E_m^*/A := \{\pm(\zeta_m^i + A) : 0 \leq i \leq \phi(m)-1\}.$$

We call $G_m(A)$ and $G_m^*(A)$ the *mth cyclotomic graph* and the *second kind mth cyclotomic graph* with respect to A, respectively.

If $A = (\alpha) \neq \{0\}$ is a principal ideal of $\mathbb{Z}[\zeta_m]$, we write $G_m(\alpha)$ and $G_m^*(\alpha)$ in place of $G_m((\alpha))$ and $G_m^*((\alpha))$, respectively.

In other words, $G_m(A)$ ($G_m^*(A)$, respectively) has vertex set $\mathbb{Z}[\zeta_m]/A$ such that $\alpha + A, \beta + A \in \mathbb{Z}[\zeta_m]/A$ are adjacent if and only if $\alpha - \beta - \zeta_m^i \in A$ or $\alpha - \beta + \zeta_m^i \in A$ for some i with $0 \leq i \leq m-1$ ($0 \leq i \leq \phi(m)-1$, respectively). Of course $G_m^*(A)$ is a spanning subgraph of $G_m(A)$.

Let us recall a few basic definitions about $\mathbb{Z}[\zeta_m]$. The *norm* of a nonzero ideal A of $\mathbb{Z}[\zeta_m]$, $N(A)$, is defined [19, Chapter 14] as the cardinality of $\mathbb{Z}[\zeta_m]/A$. For $\alpha \in \mathbb{Q}(\zeta_m)$, let $N(\alpha)$ denote the usual norm $N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)$ of α (see e.g. [19, Chapter 12]). Since $\mathbb{Q}(\zeta_m)$ is a cyclotomic number field, $N(\alpha) \geq 0$ is an integer for any $\alpha \in \mathbb{Q}(\zeta_m)$, and $N(\alpha) = 0$ if and only if $\alpha = 0$. It is well known that $N((\alpha)) = |N(\alpha)|$ (see e.g. [19, Proposition 14.1.3]).

The multiplicative group $(\mathbb{Z}[\zeta_m]/A)^*$ of units of $\mathbb{Z}[\zeta_m]/A$ acts on the additive group of $\mathbb{Z}[\zeta_m]/A$ by right multiplication: $(\alpha + A)^{\gamma + A} = (\alpha + A)(\gamma + A) = \alpha\gamma + A$. This is an action as a group because it respects the addition of $\mathbb{Z}[\zeta_m]/A$. Thus the semidirect product

$$L := (\mathbb{Z}[\zeta_m]/A) \rtimes (\mathbb{Z}[\zeta_m]/A)^*$$

is well-defined. It is straightforward to verify that

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

$$(\alpha + A)^{(\beta+A,\gamma+A)} = (\alpha + \beta)\gamma + A,\ \ \alpha + A \in \mathbb{Z}[\zeta_m]/A,\ \ (\beta + A, \gamma + A) \in L \tag{2}$$

defines a faithful action (as a set) of L on $\mathbb{Z}[\zeta_m]/A$.

The subset E_m/A of $(\mathbb{Z}[\zeta_m]/A)^*$ is a cyclic subgroup of $(\mathbb{Z}[\zeta_m]/A)^*$, which we denote by H_A. We have

$$H_A = \begin{cases} \langle(-\zeta_m) + A\rangle, & \text{if } m \text{ is odd} \\ \langle\zeta_m + A\rangle, & \text{if } m \text{ is even.} \end{cases} \tag{3}$$

In fact, if m is even, then $H_A = \langle(-\zeta_m) + A, (-1) + A\rangle = \langle\zeta_m + A, (-1) + A\rangle = \langle\zeta_m + A\rangle$ as $\zeta_m^{m/2} = -1$.

Given a generating set S of G and a cyclic permutation ρ of S, a *Cayley map* [20,30] is a 2-cell embedding of $\mathrm{Cay}(G, S)$ on an orientable surface such that for each vertex $g \in G$, the cyclic permutation of the arcs (g, sg), $s \in S$ induced by a fixed orientation of the surface coincides with ρ. A Cayley map is *balanced* [30] if $\rho(s^{-1}) = \rho(s)^{-1}$ for every $s \in S$, and *regular* if its automorphism group is regular on the set of arcs of $\mathrm{Cay}(G, S)$. It is known that the existence of a complete rotation in a Cayley graph is equivalent to the existence of a 2-cell embedding of the graph on a closed orientable surface as a balanced regular Cayley map.

Theorem 3.2. *Let $A \neq \{0\}$ be an ideal of $\mathbb{Z}[\zeta_m]$, where $m \geq 2$, and let H_A be as in (3). Then the following hold:*

(a) *$G_m(A)$ is a finite, connected, undirected graph of order $N(A)$ and valency $\mathrm{val}(G_m(A))$ a divisor of $2m$; moreover, $\mathrm{val}(G_m(A)) = 2m$ if and only if $1 \pm \zeta_m^i \notin A$ for $1 \leq i \leq m - 1$;*

(b) *under the assumption that $2 \notin A$ and m is odd, if there exists $i \geq 1$ such that $1 - \zeta_m^i \in A$, say $d \geq 1$ is the smallest integer with this property, then $\mathrm{val}(G_m(A)) = 2d$ or d, depending on whether d is odd or even with $1 + \zeta_m^{d/2} \in A$; if there exists $i \geq 1$ such that $1 + \zeta_m^i \in A$, then the smallest integer d with this property must be even and $\mathrm{val}(G_m(A)) = 2d$;*

(c) *if $2 \notin A$ and m is even, then the smallest positive integer d such that $1 - \zeta_m^d \in A$ must be even and $\mathrm{val}(G_m(A)) = d$;*

(d) *$G_m(A)$ admits $(\mathbb{Z}[\zeta_m]/A) \rtimes H_A$ as a group of automorphisms acting faithfully and transitively on the vertex set and regularly on the arc set;*

(e) *$G_m(A)$ is a rotational Cayley graph and hence can be 2-cell-embedded on a closed orientable surface as a balanced regular Cayley map.*

Proof. (a) By [19, Proposition 12.2.3], $N(A)$ is finite, that is, $G_m(A)$ is a finite graph with $N(A)$ vertices. Since H_A is closed under taking negative elements, $G_m(A)$ is an undirected graph. Since by (3), H_A is a cyclic subgroup of $(\mathbb{Z}[\zeta_m]/A)^*$ and $(-\zeta_m)^{2m} + A = \zeta_m^{2m} + A = 1 + A$, the order of H_A (that is, $\mathrm{val}(G_m(A))$) is a divisor of $2m$. By the definition of $G_m(A)$, there is at least one path in $G_m(A)$ from A to any $\alpha + A \in \mathbb{Z}[\zeta_m]/A$. (For example, if $\alpha = 2 - \zeta_m + 2\zeta_m^3$, then the sequence $A, 1 + A, 2 + A, (2 - \zeta_m) + A, (2 - \zeta_m + \zeta_m^3) + A, (2 - \zeta_m + 2\zeta_m^3) + A$ gives a path from A to $\alpha + A$.) Therefore, $G_m(A)$ is connected. It is clear that $\mathrm{val}(G_m(A)) = 2m$ if and only if $\zeta_m^i \pm \zeta_m^j \notin A$ for $0 \leq i < j \leq m - 1$, or equivalently $1 \pm \zeta_m^j \notin A$ for $1 \leq j \leq m - 1$.

(b) Suppose $2 \notin A$ and m is odd. Then $H_A = \langle(-\zeta_m) + A\rangle$.

Case 1: There exists an integer $i \geq 1$ such that $\zeta_m^i + A = 1 + A$. Let d be the smallest integer with this property. If d is even, then $H_A = \{1 + A, -\zeta_m + A, \ldots, \zeta_m^{d-2} + A, -\zeta_m^{d-1} + A\}$. Since $-1 + A \in H_A$, we have $-1 + A = -\zeta_m^{2i+1} + A$ for some $1 \leq 2i + 1 \leq d - 1$, or $-1 + A = \zeta_m^{2i} + A$ for some $1 \leq 2i \leq d - 2$ (note that $i \neq 0$ as $2 \notin A$). In the former case we obtain $1 - \zeta_m^{2i+1} \in A$, which contradicts the assumption that d is the smallest positive integer such that $1 - \zeta_m^d \in A$. In the latter case, $1 + \zeta_m^{2i} \in A$ and so $(1 + \zeta_m^{2i}) - (1 - \zeta_m^d) \in A$. This gives $1 + \zeta_m^{d-2i} \in A$ and hence $(1 + \zeta_m^{d-2i}) - (1 + \zeta_m^{2i}) = \zeta_m^{d-2i} - \zeta_m^{2i} \in A$, which contradicts the choice of d unless $d - 2i = 2i$. (In fact, if $d - 2i > 2i$, then by $\zeta_m^{d-2i} - \zeta_m^{2i} \in A$ we

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

have $1-\zeta_m^{d-4i} \in A$, contradicting the minimality of d. If $d-2i<2i$, then $1-\zeta_m^{4i-d} \in A$, which again is a contradiction as $0<4i-d \le 2(d-2)-d<d$.) In the case when $d-2i=2i$, we have $1+\zeta_m^{d/2} \in A$, $H_A=\{\pm(1+A), \pm(-\zeta_m+A), \dots, \pm(\zeta_m^{2i-2}+A), \pm(-\zeta_m^{2i-1}+A)\}$, and $G_m(A)$ has valency d. Assume d is odd. Then $H_A=\{\pm(1+A), \pm(-\zeta_m+A), \dots, \pm(-\zeta_m^{d-2}+A), \pm(\zeta_m^{d-1}+A)\}$. By the minimality of d we have $1+A \neq \zeta_m^i+A$ for $1 \le i \le d-1$. We have also $1+A \neq -1+A$ as $2 \notin A$ by our assumption. If $1+A=-\zeta_m^i+A$ for some $1 \le i \le d-1$, then $1+\zeta_m^i \in A$ and so $\zeta_m^i+\zeta_m^d=(1+\zeta_m^i)-(1-\zeta_m^d) \in A$. Thus $1+\zeta_m^{d-i} \in A$ and therefore $\zeta_m^i-\zeta_m^{d-i} \in A$, which contradicts the choice of d as $i \neq d-i$ due to d being odd.

In summary, we have proved that in Case 1 either (i) d is even, $1+\zeta_m^{d/2} \in A$ and $G_m(A)$ has valency d, or (ii) d is odd and $G_m(A)$ has valency $2d$.

Case 2: There exists an integer $i \ge 1$ such that $-\zeta_m^i+A=1+A$. Let d be the smallest integer with this property. If d is even, then $H_A=\{\pm(1+A), \pm(-\zeta_m+A), \dots, \pm(-\zeta_m^{d-2}+A), \pm(\zeta_m^{d-1}+A)\}$. Similar to the proof above, one can show that $G_m(A)$ has valency $2d$. If d is odd, then $H_A=\{1+A, -\zeta_m+A, \dots, -\zeta_m^{d-2}+A, \zeta_m^{d-1}+A\}$. Since $-1+A \in H_A$, we have $-1+A=-\zeta_m^{2i+1}+A$ for some $1 \le 2i+1 \le d-2$, or $-1+A=\zeta_m^{2i}+A$ for some $1 \le 2i \le d-1$ (note that $i \neq 0$ as $2 \notin A$). The latter case cannot happen as it contradicts the minimality of d. In the former case we obtain $\zeta_m^{2i+1}+\zeta_m^d \in A$ and so $1+\zeta_m^{d-2i-1} \in A$, which also contradicts the minimality of d.

In summary, in Case 2, d is even and $G_m(A)$ has valency $2d$.

We claim that Cases 1 and 2 coexist if and only if (i) in Case 1 occurs. In fact, let $d_1, d_2 \ge 1$ be the smallest integers such that $1-\zeta_m^{d_1}, 1+\zeta_m^{d_2} \in A$. Then $\zeta_m^{d_1}+\zeta_m^{d_2} \in A$ and so $1+\zeta_m^{d_2-d_1}, 1+\zeta_m^{d_1-d_2} \in A$. By the minimality of d_2, we have $d_1 \ge 2d_2$. We also have $\zeta_m^{d_2}-\zeta_m^{d_1-d_2}=(1+\zeta_m^{d_2})-(1+\zeta_m^{d_1-d_2}) \in A$ and so $1-\zeta_m^{d_1-2d_2} \in A$. By the minimality of d_1, we have $d_1=2d_2$, yielding (i) in Case 1.

(c) Suppose $2 \notin A$ and m is even. Then $H_A=\langle \zeta_m+A \rangle$. Let d be the smallest positive integer such that $\zeta_m^d+A=1+A$. (The existence of d is ensured by the fact that $\zeta_m^m+A=1+A$.) Then $H_A=\{1+A, \zeta_m+A, \dots, \zeta_m^{d-2}+A, \zeta_m^{d-1}+A\}$ and $-1+A=\zeta_m^i+A$ for some $1 \le i \le d-1$ (note that $i \neq 0$ as $2 \notin A$). So $\zeta_m^i+\zeta_m^d \in A$ and $1+\zeta_m^{d-i} \in A$, which together with $1+\zeta_m^i \in A$ implies $\zeta_m^i-\zeta_m^{d-i} \in A$. This together with the minimality of d implies that $d=2i$ and hence $H_A=\{\pm(1+A), \pm(\zeta_m+A), \dots, \pm(\zeta_m^{i-1}+A)\}$. It follows that $G_m(A)$ has valency d.

(d) Since H_A is a subgroup of $(\mathbb{Z}[\zeta_m]/A)^*$, the semidirect product

$$H := (\mathbb{Z}[\zeta_m]/A) \rtimes H_A$$

is a well-defined subgroup of L. Since L is faithful on $\mathbb{Z}[\zeta_m]/A$, so is H. We claim that H preserves the adjacency and non-adjacency relations of $G_m(A)$. In fact, the images of $\alpha_1+A, \alpha_2+A \in \mathbb{Z}[\zeta_m]/A$ under $(\beta+A, \pm(\zeta_m^i+A)) \in H$ are $\pm((\alpha_1+\beta)\zeta_m^i+A)$ and $\pm((\alpha_2+\beta)\zeta_m^i+A)$, respectively. Since the difference between these two elements is $\pm((\alpha_1-\alpha_2)\zeta_m^i+A)$, it follows from the definition of $G_m(A)$ that α_1+A and α_2+A are adjacent in $G_m(A)$ if and only if their images under $(\beta+A, \pm(\zeta_m^i+A))$ are adjacent in $G_m(A)$. Therefore, H respects the adjacency and non-adjacency relations of $G_m(A)$. Thus $G_m(A)$ admits H as a group of automorphisms acting faithfully on the vertex set. The subgroup $\mathbb{Z}[\zeta_m]/A$ of H is transitive on $\mathbb{Z}[\zeta_m]/A$ by addition, and so H is transitive on the vertex set of $G_m(A)$. In view of (2), the image of $A \in \mathbb{Z}[\zeta_m]/A$ under $(\beta+A, \pm(\zeta_m^i+A))$ is $\pm(\beta\zeta_m^i+A)$, which is equal to A if and only if $\beta \in A$. Thus the stabilizer of the vertex A of $G_m(A)$ under the action of H is the subgroup

$$H_A^* := \{(A, \pm(\zeta_m^i+A)) : 0 \le i \le m-1\}$$

of H, which is isomorphic to H_A. It follows that this stabilizer is transitive on the neighbourhood E_m/A of A in $G_m(A)$, because $(\varepsilon\zeta_m^i+A)^{(\beta+A, \varepsilon'\zeta_m^j+A)}=\pm(\zeta_m^{i+j}+A)$ (where $\varepsilon, \varepsilon'=\pm 1$) by (2). This together with the vertex-transitivity of H on $\mathbb{Z}[\zeta_m]/A$ implies that H is transitive on the arc set of $G_m(A)$. Moreover, by the orbit-stabiliser lemma, the order of H is equal to $N(A) \cdot |H_A^*| = N(A) \cdot \mathrm{val}(G_m(A))$, which is the number of arcs of $G_m(A)$. Therefore, H must be regular on the arc set of $G_m(A)$.

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

(e) In the case when m is odd, $(A, (-\zeta_m) + A) \in H_A^*$ generates the cyclic group H_A^*, fixes setwise the neighbourhood $E_m/A = \{(-\zeta_m)^i + A : 0 \le i \le 2m-1\}$ of A, and permutes the neighbours of A in a cyclic manner by $((-\zeta_m)^i + A)^{(A,(-\zeta_m)+A)} = (-\zeta_m)^{i+1} + A$, $0 \le i \le 2m-1$. Therefore, $(A, (-\zeta_m) + A)$ is a complete rotation of $G_m(A)$ and hence $G_m(A)$ can be 2-cell-embedded on a closed orientable surface as a balanced regular Cayley map. Similarly, when m is even, the same result holds with $(A, \zeta_m + A)$ a complete rotation of $G_m(A)$. □

Remark 3.3. Choose $\zeta_3 = -\rho := -(1+\sqrt{-3})/2$ so that $\rho^2 - \rho + 1 = 0$. Then $\mathbb{Z}[\rho] = \{x + y\rho : x, y \in \mathbb{Z}\}$ is the ring of *Eisenstein–Jacobi integers* with norm defined by $N(x + y\rho) = x^2 + xy + y^2$. It is known that $\mathbb{Z}[\rho]^* = \langle \rho \rangle = \{\pm\rho^i : i = 0, 1, 2\}$. Since $\mathbb{Z}[\rho]$ is an Euclidean domain, every nonzero ideal of it is a principal ideal (α), and $G_3(\alpha)$ is precisely the *Eisenstein–Jacobi (EJ) graph* EJ_α [24]. (Unlike [24, Definition 19], we do not require $\gcd(a, b) = 1$ in $EJ_{a+b\rho}$. In [24] the EJ graph $EJ_{a+b\omega}$ was defined as the Cayley graph on (the additive group of) $\mathbb{Z}[\omega]/(a + b\omega)$ with respect to $\{\pm(1 + (a + b\omega)), \pm(\omega + (a + b\omega)), \pm(\omega^2 + (a + b\omega))\}$, where $\omega = (-1 + \sqrt{-3})/2$. As noted in [13], although $EJ_{a+b\omega}$ has $a^2 - ab + b^2$ vertices and is different from $EJ_{a+b\rho}$, the family of EJ graphs is the same no matter whether $\mathbb{Z}[\rho]$ or $\mathbb{Z}[\omega]$ is used.)

In the case when $m = 4$, we choose $\zeta_4 = i$ (the imaginary unit) and so $\mathbb{Z}[\zeta_4]$ is the ring of Gaussian integers $\mathbb{Z}[i]$ with norm defined by $N(x + yi) = x^2 + y^2$. Let $0 \ne \alpha = a + bi \in \mathbb{Z}[i]$ be such that $N(\alpha) \ge 5$. Then $G_4(\alpha) = G_4^*(\alpha)$ is exactly the *Gaussian network* G_α introduced in [24].

4. Perfect codes in cyclotomic graphs

Let $\alpha = \sum_{i=0}^{\phi(m)-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$, where $a_i \in \mathbb{Z}$. Define [10]

$$|\alpha| := \sum_{i=0}^{\phi(m)-1} |a_i|,$$

where $|a_i|$ denotes the usual absolute value of a_i. This defines an integer-valued weight function on $\mathbb{Z}[\zeta_m]$, called the *Manhattan weight* [18] on $\mathbb{Z}[\zeta_m]$. This weight then defines the *Manhattan distance* $|\alpha - \beta|$ between α and β; this is a distance function because it is nonnegative, symmetric and satisfies the triangle inequality (see [10]).

Denote $\alpha + A$ by $\bar{\alpha}$ for $\alpha \in \mathbb{Z}[\zeta_m]$ (and in particular $\bar{0} = 0 + A$). Define

$$\|\bar{\alpha}\| := \min\{|\alpha - \delta| : \delta \in A\}. \tag{4}$$

Note that both $\bar{\alpha}$ and $\|\bar{\alpha}\|$ rely on A. Note also that $\|\bar{\alpha}\|$ is independent of the choice of the representative α in $\alpha + A$. It was proved in [10, Section II-D] that this defines an integer-valued weight on $\mathbb{Z}[\zeta_m]/A$, that is, (i) $\|\bar{\alpha}\| \ge 0$ with equality if and only if $\bar{\alpha} = \bar{0}$, (ii) $\|\bar{\alpha}\| = \|-\bar{\alpha}\|$, and (iii) $\|\bar{\alpha} + \bar{\beta}\| \le \|\bar{\alpha}\| + \|\bar{\beta}\|$. This weight then defines the distance $\|\bar{\alpha} - \bar{\beta}\|$ between $\bar{\alpha}$ and $\bar{\beta}$, called the *Mannheim distance* [10,18]. (This notion was introduced in [10] when A is a prime ideal, but it works well for any nonzero ideal A of $\mathbb{Z}[\zeta_m]$.)

We now show that the Mannheim distance gives the distance between vertices in $G_m^*(A)$. This observation is crucial for us to understand perfect codes in $G_m^*(A)$.

Lemma 4.1. *Let $m \ge 2$ be an integer and A a nonzero proper ideal of $\mathbb{Z}[\zeta_m]$. Then for any $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}[\zeta_m]/A$ the distance in $G_m^*(A)$ between $\bar{\alpha}$ and $\bar{\beta}$ is equal to $\|\bar{\alpha} - \bar{\beta}\|$.*

Proof. Since $A \ne \mathbb{Z}[\zeta_m]$, we have $\zeta_m^i \notin A$ for each integer i.

We first show that $\bar{\alpha}$ and $\bar{\beta}$ are adjacent in $G_m^*(A)$ if and only if $\|\bar{\alpha} - \bar{\beta}\| = 1$. In fact, if $\bar{\alpha}$ and $\bar{\beta}$ are adjacent in $G_m^*(A)$, then $(\alpha - \beta) \pm \zeta_m^i \in A$ for some $0 \le i \le \phi(m) - 1$, and hence $\|\bar{\alpha} - \bar{\beta}\| = \min\{|\zeta_m^i - \delta| :$

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

$\delta \in A\} \leq |\zeta_m^i| = 1$. However, $\|\bar{\alpha} - \bar{\beta}\| \geq 1$ as $\bar{\alpha} \neq \bar{\beta}$. Therefore, $\|\bar{\alpha} - \bar{\beta}\| = 1$. Conversely, if $\|\bar{\alpha} - \bar{\beta}\| = 1$, then there exists $\delta \in A$ such that $|(\alpha - \beta) - \delta| = 1$ and so $(\alpha - \beta) - \delta = \pm\zeta_m^i$ for some $0 \leq i \leq \phi(m) - 1$, implying that $\bar{\alpha}$ and $\bar{\beta}$ are adjacent in $G_m^*(A)$.

In general, let $s = \|\bar{\alpha} - \bar{\beta}\|$ and let $t = d(\bar{\alpha}, \bar{\beta})$ be the distance between $\bar{\alpha}$ and $\bar{\beta}$ in $G_m^*(A)$. Let $\bar{\alpha} = \bar{\alpha}_0, \bar{\alpha}_1, \ldots, \bar{\alpha}_t = \bar{\beta}$ be a shortest path in $G_m^*(A)$. Since $\bar{\alpha}_i$ and $\bar{\alpha}_{i+1}$ are adjacent in $G_m^*(A)$, we have $\|\bar{\alpha}_i - \bar{\alpha}_{i+1}\| = 1$ by what we proved in the previous paragraph. Since $\bar{\alpha} - \bar{\beta} = \sum_{i=0}^{t-1}(\bar{\alpha}_i - \bar{\alpha}_{i+1})$, we obtain $s = \|\bar{\alpha} - \bar{\beta}\| \leq t$ by the triangular inequality.

In view of (4), there exists $\delta \in A$ such that $s = |(\alpha - \beta) - \delta|$. So we may write $(\alpha - \beta) - \delta = c_{i_1}\zeta_m^{i_1} + \cdots + c_{i_k}\zeta_m^{i_k} - (d_{j_1}\zeta_m^{j_1} + \cdots + d_{j_l}\zeta_m^{j_l})$, where $i_1, \ldots, i_k, j_1, \ldots, j_l$ are pairwise distinct integers between 0 and $\phi(m) - 1$ and $c_{i_1}, \ldots, c_{i_k}, d_{j_1}, \ldots, d_{j_l}$ are positive integers summing up to s. Thus the sequence

$$A, \zeta_m^{i_1} + A, \ldots, c_{i_1}\zeta_m^{i_1} + A, (c_{i_1}\zeta_m^{i_1} + \zeta_m^{i_2}) + A, \ldots, (c_{i_1}\zeta_m^{i_1} + c_{i_2}\zeta_m^{i_2}) + A, \ldots, ((\alpha - \beta) - \delta) + A$$

is a path in $G_m^*(A)$ with length $c_{i_1} + \cdots + c_{i_k} + d_{j_1} + \cdots + d_{j_l} = s$. (In each step of the sequence there is an increase or decrease by some $\zeta_m^{i_r}$.) Since $((\alpha - \beta) - \delta) + A = (\alpha + A) - (\beta + A)$ (as $\delta \in A$), this sequence gives a path in $G_m^*(A)$ between $\bar{0}$ and $\bar{\alpha} - \bar{\beta}$ and hence $d(\bar{0}, \bar{\alpha} - \bar{\beta}) \leq s$. However, we have $d(\bar{\alpha}, \bar{\beta}) = d(\bar{0}, \bar{\alpha} - \bar{\beta})$ because the additive group of $\mathbb{Z}[\zeta_m]/A$ is regular on the vertex set $\mathbb{Z}[\zeta_m]/A$ of $G_m^*(A)$ by addition as a group of automorphisms. Therefore, $t \leq s$ and the proof is complete. □

Denote by $B_t(\bar{\beta})$ and $B_t^*(\bar{\beta})$ the t-neighbourhood of $\bar{\beta} \in \mathbb{Z}[\zeta_m]/A$ in $G_m(A)$ and $G_m^*(A)$, respectively. Since $G_m(A)$ and $G_m^*(A)$ are both vertex-transitive, we have $|B_t(\bar{\beta})| = |B_t(\bar{0})|$ and $|B_t^*(\bar{\beta})| = |B_t^*(\bar{0})|$ for all $\bar{\beta} \in \mathbb{Z}[\zeta_m]/A$. By Lemma 4.1,

$$B_t^*(\bar{\beta}) = \{\bar{\gamma} \in \mathbb{Z}[\zeta_m]/A : \|\bar{\beta} - \bar{\gamma}\| \leq t\}.$$

Note that, if D is an ideal of $\mathbb{Z}[\zeta_m]$ containing A, then $D/A = \{\beta + A : \beta \in D\}$ is a subring of $\mathbb{Z}[\zeta_m]/A$. The following result easily follows from Lemma 4.1 and the definition of a perfect code.

Lemma 4.2. *Let $m \geq 2$ and $t \geq 1$ be integers, and let A and D be nonzero ideals of $\mathbb{Z}[\zeta_m]$ such that $A \subseteq D$. Then the following hold:*

(a) *D/A is a perfect t-code in $G_m^*(A)$ if and only if*

$$|B_t^*(\bar{0})| = N(D)$$

and

$$|\eta - \delta| \geq 2t + 1 \tag{5}$$

for any $\delta \in A$ and $\eta \in D - A$;

(b) *D/A is a perfect t-code in $G_m(A)$ only when*

$$|B_t(\bar{0})| = N(D)$$

and (5) holds for any $\delta \in A$ and $\eta \in D - A$.

Proof. By Lemma 4.1, we have: $B_t^*(\bar{\beta}) \cap B_t^*(\bar{\gamma}) = \emptyset$ for distinct $\bar{\beta}, \bar{\gamma} \in D/A \Leftrightarrow \|\bar{\beta} - \bar{\gamma}\| \geq 2t + 1$ for distinct $\bar{\beta}, \bar{\gamma} \in D/A \Leftrightarrow \|\bar{\eta}\| \geq 2t + 1$ for any $\bar{0} \neq \bar{\eta} \in D/A \Leftrightarrow |\eta - \delta| \geq 2t + 1$ for any $\delta \in A$ and $\eta \in D - A$. We have $|D/A| = N(A)/N(D)$ as $(\mathbb{Z}[\zeta_m]/A)/(D/A) \cong \mathbb{Z}[\zeta_m]/D$.

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

Using the facts above, we have: D/A is a perfect t-code in $G_m^*(A) \Leftrightarrow \{B_t^*(\bar{\beta}) : \bar{\beta} \in D/A\}$ is a partition of $\mathbb{Z}[\zeta_m]/A \Leftrightarrow |D/A| \cdot |B_t^*(\bar{\beta})| = N(A)$ and $B_t^*(\bar{\beta}) \cap B_t^*(\bar{\gamma}) = \emptyset$ for distinct $\bar{\beta}, \bar{\gamma} \in D/A \Leftrightarrow |B_t^*(\bar{0})| = N(D)$ and (5) holds for any $\delta \in A$ and $\eta \in D - A$.

Since $G_m^*(A)$ is a spanning subgraph of $G_m(A)$, we have $B_t^*(\bar{\beta}) \subseteq B_t(\bar{\beta})$ for any $\bar{\beta} \in \mathbb{Z}[\zeta_m]/A$. Thus we have: D/A is a perfect t-code in $G_m(A) \Leftrightarrow \{B_t(\bar{\beta}) : \bar{\beta} \in D/A\}$ is a partition of $\mathbb{Z}[\zeta_m]/A \Leftrightarrow |D/A| \cdot |B_t(\bar{\beta})| = N(A)$ and $B_t(\bar{\beta}) \cap B_t(\bar{\gamma}) = \emptyset$ for distinct $\bar{\beta}, \bar{\gamma} \in D/A \Rightarrow |B_t(\bar{0})| = N(D)$ and $B_t^*(\bar{\beta}) \cap B_t^*(\bar{\gamma}) = \emptyset$ for distinct $\bar{\beta}, \bar{\gamma} \in D/A \Rightarrow |B_t(\bar{0})| = N(D)$ and (5) holds for any $\delta \in A$ and $\eta \in D - A$. □

The following is an immediate consequence of Lemma 4.2.

Corollary 4.3. *Let $m \geq 2$ and $t \geq 1$ be integers, and let $0 \neq \alpha, \beta \in \mathbb{Z}[\zeta_m]$ be such that β divides α. Then the following hold:*

(a) *$(\beta)/(\alpha)$ is a perfect t-code in $G_m^*(\alpha)$ if and only if*

$$|B_t^*(\bar{0})| = N(\beta) \tag{6}$$

and

$$|\tau\beta| \geq 2t + 1 \tag{7}$$

for any nonzero $\tau \in \mathbb{Z}[\zeta_m]$;

(b) *$(\beta)/(\alpha)$ is a perfect t-code in $G_m(\alpha)$ only when*

$$|B_t(\bar{0})| = N(\beta) \tag{8}$$

and (7) holds any nonzero $\tau \in \mathbb{Z}[\zeta_m]$.

Remark 4.4. Lemma 4.2 and Corollary 4.3 only provide necessary conditions for D/A and $(\beta)/(\alpha)$ to be a perfect t-code in $G_m(A)$ and $G_m(\alpha)$, respectively. We are unable to tell whether these conditions are sufficient due to lack of knowledge of the distance in $G_m(A)$ and $G_m(\alpha)$. In general, this distance is not the Mannheim distance as observed in [13,24] for $m = 3, 4$.

In the special case when $m = 3, 4$, by using Corollary 4.3 and the knowledge of the distance in $G_m(A)$ [13,26], we now prove that two sufficient conditions given in [24,26] are also necessary.

As mentioned in Remark 3.3, for $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ with $N(\alpha) \geq 5$, $G_4(\alpha)$ is the Gaussian network G_α introduced in [24]. It can be easily seen that $G_\alpha \cong G_{i\alpha^j}$ for any integer j. So we may assume $a, b \geq 0$ in subsequent discussion about Gaussian networks. The size of the ball $B_t(\bar{0})$ of radius t around $\bar{0} = 0 + (\alpha)$ in G_α was determined in [26] for any $t \geq 0$. In particular, it was proved in [26, Theorems 10-11] that, if $0 \leq a \leq b$, then

$$|B_t(\bar{0})| = 4t, \ \ 0 \leq t \leq \lfloor (a + b - 1)/2 \rfloor. \tag{9}$$

In fact, this formula is also valid when $a > b \geq 0$ as $G_{a+bi} \cong G_{b+ai}$ (see [13, Section IV]). It is known that two elements β, γ of $\mathbb{Z}[i]$ are associates of each other if and only if $\beta = i^j\gamma$ for some integer j. Since $\mathbb{Z}[i]$ is a principal ideal domain and associates generate the same principal ideal, any nonzero ideal of $\mathbb{Z}[i]$ is of the form $(c + di)$ or $(c - di)$ for some $c, d \geq 0$.

The 'if' part of the following result was proved in [26, Theorem 18], which improved an earlier version [24, Theorem 14] that required the extra condition $\gcd(a, b) = 1$. We complete the picture by proving the

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

'only if' part by using Corollary 4.3(b). (Note that the condition $t \le \lfloor (a+b-1)/2 \rfloor$ is needed for otherwise $(\beta)/(\alpha)$ may not be a perfect t-code in G_α.)

Theorem 4.5. *Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ (where $a, b \ge 0$), and let $0 \neq \beta \in \mathbb{Z}[i]$ be such that $N(\alpha) \ge 5$ and β divides α. Let t be an integer between 1 and $\lfloor (a+b-1)/2 \rfloor$. Then $(\beta)/(\alpha)$ is a perfect t-code in G_α if and only if β is an associate of $t + (t+1)i$ or $t - (t+1)i$.*

Proof. We only need to prove the necessity. As mentioned above, we may assume $0 \neq \beta = c \pm di \in \mathbb{Z}[i]$, where $c, d \ge 0$. Since β divides α, we have $(\alpha) \subseteq (\beta)$, $\alpha = \gamma\beta$ for some $\gamma \in \mathbb{Z}[i]$, and $N(\beta) = c^2 + d^2$ divides $N(\alpha) = a^2 + b^2$. Since $N(\alpha) \ge 5$, G_α has valency 4 by Theorem 3.2(c). Since $1 \le t \le \lfloor (a+b-1)/2 \rfloor$, by (9), $|B_t(\bar{0})| = 1 + 4\sum_{j=1}^{t} j = 2t(t+1) + 1$.

Suppose that $(\beta)/(\alpha)$ is a perfect t-code in G_α. Then by (8) we have $c^2 + d^2 = 2t(t+1) + 1$, and by (7), $|\tau\beta| \ge 2t + 1$ for any $0 \neq \tau \in \mathbb{Z}[i]$. Since $|i^j \tau\beta| = |\tau\beta|$ for any integer j, by multiplying τ by i, i^2 or i^3 when necessary, we may assume that $\tau = f \pm gi$ where $f, g \ge 0$ with $(f, g) \neq (0, 0)$. Note that $\tau\beta = (cf \mp dg) + (df \pm cg)i$ when $\beta = c + di$ and $\tau\beta = (cf \pm dg) - (df \mp cg)i$ when $\beta = c - di$. In both cases, (7) is equivalent to

$$|cf - dg| + |df + cg| \ge 2t + 1, \quad |cf + dg| + |df - cg| \ge 2t + 1 \tag{10}$$

for any integers $f, g \ge 0$ with $(f, g) \neq (0, 0)$.

Assume $c \ge d$ first. Choosing $(f, g) = (1, 1)$ in (10), we obtain $2c \ge 2t + 1$ and so $c \ge t + 1$. This together with $c^2 + d^2 = 2t(t+1) + 1$ implies $d \le t$. Choosing $(f, g) = (1, 0)$ in (10), we obtain $c + d \ge 2t + 1$. If $c + d > 2t + 1$, then $2t(t+1) + 1 = c^2 + d^2 > ((2t+1) - d)^2 + d^2$, yielding $0 > (d - t)(d - (t+1))$. However, this cannot happen as $d \le t$. Hence $c + d = 2t + 1$. Combining this with $c^2 + d^2 = 2t(t+1) + 1$, we obtain $cd = t(t+1)$. Therefore the only possibility is that $c = t + 1$ and $d = t$.

Now assume $c < d$. Setting $(f, g) = (1, 1)$ in (10), we have $2d \ge 2t + 1$ and so $d \ge t + 1$. This together with $c^2 + d^2 = 2t(t+1) + 1$ implies $c \le t$. Choosing $(f, g) = (1, 0)$ in (10), we obtain $c + d \ge 2t + 1$. Similar to the argument above, we then obtain $c = t$ and $d = t + 1$.

We conclude the proof by noting that $(t+1) + ti = i(t - (t+1)i)$ and $(t+1) - ti = i^3(t + (t+1)i)$. □

Remark 4.6. Theorem 4.5 can be restated as follows: Let $\beta = t \pm (t+1)i$ with t a positive integer. Then for any $\alpha = (x + yi)\beta$ or $(x - yi)\beta$, where $x, y \ge 0$, $(x, y) \neq (0, 0)$, G_α has $(\beta)/(\alpha)$ as a perfect t-code. Moreover, up to isomorphism these are the only cyclotomic graphs G_γ with β dividing γ that admit $(\beta)/(\gamma)$ as a perfect t-code in G_γ.

We now move on to the third cyclotomic graphs $EJ_\alpha = G_3(\alpha)$ (see Remark 3.3), where $0 \neq \alpha = a + b\rho$ and $\rho = (1 + \sqrt{-3})/2$. Since $G_\alpha \cong G_{\rho^j \alpha}$ for any integer j, without loss of generality we may assume $a, b \ge 0$ in EJ_α. The size of the ball $B_t(\bar{0})$ of radius t around $\bar{0} = 0 + (\alpha)$ in EJ_α was determined in [13] for any $t \ge 0$. In particular, it was proved in [13, Theorem 27] that, if $a \ge b \ge 0$, then

$$|B_t(\bar{0})| = 6t, \ \ 0 \le t < (a+b)/2. \tag{11}$$

Note that this formula is also valid when $0 \le a < b$ as $G_{a+b\rho} \cong G_{b+a\rho}$ (see [13, Section IV]). It is known that two elements β, γ of $\mathbb{Z}[\rho]$ are associates of each other if and only if $\beta = \rho^j \gamma$ for some integer j. Since $\mathbb{Z}[\rho]$ is a principal ideal domain and associates generate the same principal ideal, any nonzero ideal of $\mathbb{Z}[\rho]$ is of the form $(c + d\rho)$ or $(c - d\rho)$ for some integers $c, d \ge 0$.

In [13, Section IV], the *ρ-taxicab norm* of $\gamma \in \mathbb{Z}[\rho]$ was defined as

$$|\gamma|_\rho := \min\{|x| + |y| + |z| : \gamma = x + y\rho + z\rho^2, \ x, y, z \in \mathbb{Z}\}$$

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

and the *EJ-norm* of $\bar{\gamma} = \gamma + (\alpha)$ in EJ_α was defined as

$$\|\bar{\gamma}\|_E := \min\{|\gamma - \eta\alpha|_\rho : \eta \in \mathbb{Z}[\rho]\}.$$

Since $\|\bar{\gamma}_1\|_E = \|\bar{\gamma}_2\|_E$ whenever $\gamma_1 \equiv \gamma_2 \bmod \alpha$, $\|\bar{\gamma}\|_E$ is well-defined. It was proved in [13, Section IV] (see also [24]) that the distance in EJ_α between $\bar{\beta}$ and $\bar{\gamma}$ is given by $\|\bar{\beta} - \bar{\gamma}\|_E$.

The 'if' part of the next result was proved in [24, Theorem 24] under the assumption $\gcd(a, b) = 1$. (Note that in [24, Theorem 24] β has a different form due to the usage of $\omega = (-1+\sqrt{-3})/2$ there.) We now show that the condition $\gcd(a, b) = 1$ can be removed, by using [13, Theorem 27] and the argument in the proof of [24, Theorem 24]. Moreover, by using Corollary 4.3(b), we prove that the 'only if' part is also true.

Theorem 4.7. *Let $0 \neq \alpha = a + b\rho \in \mathbb{Z}[\rho]$ (where $a, b \geq 0$), and let $0 \neq \beta \in \mathbb{Z}[\rho]$ be such that $N(\alpha) \geq 7$ and β divides α. Let t be an integer between 1 and $\lfloor (a + b - 1)/2 \rfloor$. Then $(\beta)/(\alpha)$ is a perfect t-code in EJ_α if and only if β is an associate of $(t + 1) + t\rho$ or $t + (t + 1)\rho$.*

Proof. As noted above, we may assume $0 \neq \beta = c \pm d\rho \in \mathbb{Z}[\rho]$, where $c, d \geq 0$. Since β divides α, we have $(\alpha) \subseteq (\beta)$, $\alpha = \gamma\beta$ for some $\gamma \in \mathbb{Z}[i]$, and $N(\beta) = c^2 \pm cd + d^2$ divides $N(\alpha) = a^2 + ab + b^2$. Since $N(\alpha) \geq 7$, EJ_α has valency 6 by Theorem 3.2(b). Since $1 \leq t \leq (a + b - 1)/2$, by (11), $|B_t(\bar{0})| = 1 + 6\sum_{j=1}^{t} j = 3t(t + 1) + 1$.

Necessity. Suppose that $(\beta)/(\alpha)$ is a perfect t-code in EJ_α. Then by (8), $c^2 \pm cd + d^2 = 3t(t + 1) + 1$, and by (7), $|\tau\beta| \geq 2t + 1$ for every $0 \neq \tau \in \mathbb{Z}[\rho]$. Since $|\rho^j\tau\beta| = |\tau\beta|$ for any integer j, multiplying τ by an appropriate ρ^j when necessary we may assume $\tau = f \pm g\rho$, where $f, g \geq 0$ with $(f, g) \neq (0, 0)$. Note that $\tau\beta = cf + (df \pm cg)\rho \pm dg\rho^2 = (cf \mp dg) + (df \pm (c+d)g)\rho$ when $\beta = c + d\rho$, and $\tau\beta = cf - (df \mp cg)\rho \mp dg\rho^2 = (cf \pm dg) - (df \mp (c - d)g)\rho$ when $\beta = c - d\rho$.

Case 1: $\beta = c + d\rho$. In this case, $c^2 + cd + d^2 = 3t(t + 1) + 1$ by (8), and (7) is equivalent to

$$|cf - dg| + |df + (c + d)g| \geq 2t + 1, \quad |cf + dg| + |df - (c + d)g| \geq 2t + 1 \tag{12}$$

for any integers $f, g \geq 0$ with $(f, g) \neq (0, 0)$. Setting $(f, g) = (1, 0)$, we obtain $c + d \geq 2t + 1$.

Assume $c \geq d$ first. In this case we have $c \geq t + 1$ as $c + d \geq 2t + 1$. This together with $c^2 + cd + d^2 = 3t(t + 1) + 1$ implies

$$\begin{aligned} d &= \tfrac{1}{2}\left(-c + \sqrt{4(3t(t + 1) + 1) - 3c^2}\right) \\ &\leq \tfrac{1}{2}\left(-(t + 1) + \sqrt{4(3t(t + 1) + 1) - 3(t + 1)^2}\right) \\ &= t. \end{aligned}$$

If $c + d > 2t + 1$, then $3t(t + 1) + 1 = c^2 + cd + d^2 > ((2t + 1) - d)^2 + ((2t + 1) - d)d + d^2$, yielding $0 > (d - t)(d - (t + 1))$. Since this contradicts the fact $d \leq t$, we must have $c + d = 2t + 1$. This together with $c^2 + cd + d^2 = 3t(t + 1) + 1$ implies $cd = t(t + 1)$. Therefore, $(c, d) = (t + 1, t)$.

Now assume $c < d$. Then $2d > c + d \geq 2t + 1$ and so $d \geq t + 1$. Similar to the previous paragraph, we then have $c \leq t$ and based on this we can further prove that $(c, d) = (t, t + 1)$.

Case 2: $\beta = c - d\rho$. In this case, $c^2 - cd + d^2 = 3t(t + 1) + 1$ by (8), and (7) is equivalent to

$$|cf + dg| + |df - (c - d)g| \geq 2t + 1, \quad |cf - dg| + |df + (c - d)g| \geq 2t + 1 \tag{13}$$

for any integers $f, g \geq 0$ with $(f, g) \neq (0, 0)$.

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

Assume $c \geq d$ first. Since $c^2 - cd + d^2 = 3t(t+1)+1$, we have

$$d = \frac{1}{2}\left(c \pm \sqrt{4(3t(t+1)+1) - 3c^2}\right). \tag{14}$$

Since d is a real number, we have $3c^2 \leq 4(3t(t+1)+1) = 3(2t+1)^2 + 1$, which implies $c \leq 2t+1$. On the other hand, setting $(f,g) = (0,1)$ in (13), we obtain $c = d + |c-d| \geq 2t+1$. Hence $c = 2t+1$. Plugging this into (14), we obtain $d = t+1$ or t. Therefore, $(c,d) = (2t+1, t+1)$ or $(2t+1, t)$.

Next assume $c < d$. Similar to (13), we have

$$c = \frac{1}{2}\left(d \pm \sqrt{4(3t(t+1)+1) - 3d^2}\right), \tag{15}$$

which implies $d \leq 2t+1$. On the other hand, setting $(f,g) = (1,1)$ in (13), we obtain $d = |c-d| + |d+(c-d)| \geq 2t+1$. Hence $d = 2t+1$. Plugging this into (15), we obtain $c = t+1$ or t. Therefore, $(c,d) = (t+1, 2t+1)$ or $(t, 2t+1)$.

It can be verified that $(2t+1)-(t+1)\rho = \rho^5[(t+1)+t\rho]$, $(2t+1)-t\rho = \rho^5[t+(t+1)\rho]$, $(t+1)-(2t+1)\rho = \rho^4[t+(t+1)\rho]$ and $t-(2t+1)\rho = \rho^4[(t+1)+t\rho]$. So the ideals (β) in Case 2 give rise to the same perfect t-codes as in Case 1.

Sufficiency: We use essentially the same argument as in the proof of [24, Theorem 24], but we do not require $\gcd(a,b) = 1$. Suppose first that $\beta = (t+1)+t\rho$ divides α. We aim to prove that $(\beta)/(\alpha)$ is a perfect t-code in EJ_α. Since $|B_t(\bar{0})| = N(\beta) = 3t(t+1)+1$, it suffices to prove that the distance $\|\bar{\gamma} - \bar{\delta}\|_E$ in EJ_α between any two vertices $\bar{\gamma}, \bar{\delta} \in (\beta)/(\alpha)$ is at least $2t+1$ (see the proof of Lemma 4.2), or equivalently, $\|\overline{\gamma\beta}\|_E \geq 2t+1$ for any $0 \neq \gamma \in \mathbb{Z}[\rho]$. Suppose otherwise. Since β divides α, there exist $0 \neq \eta \in \mathbb{Z}[\rho]$ and integers x, y, z such that $\eta\beta = x + y\rho + z\rho^2$ and $\|\overline{\gamma\beta}\|_E = |x| + |y| + |z| \leq 2t$. Set $\eta = f + g\rho$, where $(f,g) \neq (0,0)$ are integers. Then $\eta\beta = (f(t+1) - gt) + (ft + g(2t+1))\rho$. On the other hand, we have $\eta\beta = (x-z) + (y+z)\rho$. Hence $x - z = f(t+1) - gt$, $y + z = ft + g(2t+1)$ and $x + y = f(2t+1) + g(t+1)$. It follows that $|x| + |z| \geq |f(t+1) - gt|$, $|y| + |z| \geq |ft + g(2t+1)|$ and $|x| + |y| \geq |f(2t+1) + g(t+1)|$. Thus, if $|f| < |g|$, then $|y| + |z| \geq |g(2t+1)| - |ft| \geq (|f|+1)(2t+1) - |f|t \geq 2t+1$. Similarly, if $|f| > |g|$, then $|x| + |y| \geq 2t+1$. Moreover, if $f = g \neq 0$ then $|x| + |y| \geq 2t+1$, and if $f = -g \neq 0$ then $|x| + |z| \geq 2t+1$. In any case, we have $|x| + |y| + |z| \geq 2t+1$, a contradiction. Therefore, the distance in EJ_α between any two distinct vertices of $(\beta)/(\alpha)$ is at least $2t+1$. Consequently, the balls $B_t(\bar{\gamma})$, $\bar{\gamma} \in (\beta)/(\alpha)$ are pairwise disjoint. However, there are $N(\alpha)/N(\beta)$ such balls and each of them has size $N(\beta)$. Therefore, these balls form a partition of the vertex set $\mathbb{Z}[\rho]/(\alpha)$ of EJ_α. That is, $(\beta)/(\alpha)$ is a perfect t-code in EJ_α.

It can be verified that, for $\beta = t+(t+1)\rho$ and $\eta = f+g\rho$, we have $\eta\beta = (ft - g(t+1)) + (f(t+1) + g(2t+1))\rho$. Using this and a similar argument as above, one can show that $(\beta)/(\alpha)$ is a perfect t-code in EJ_α provided that β divides α. □

5. Circulant cyclotomic graphs

In this section we present a family of circulant cyclotomic graphs of valency twice an odd prime, namely $2p$-valent first kind Frobenius circulants. We give a classification of all such graphs in Theorem 5.3 and then prove that they are indeed cyclotomic in Theorem 5.5.

Since $\mathbb{Z}[\zeta_m]$ is a $\mathbb{Z}$-module with integral basis $1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}$, we may write

$$\zeta_m^i = \sum_{j=0}^{\phi(m)-1} c_{ij}\zeta_m^j,\ 0 \leq i \leq m-1, \tag{16}$$

where all $c_{ij} \in \mathbb{Z}$ are determined by ζ_m. Note that, for $0 \leq i \leq \phi(m)-1$, we have $c_{ii} = 1$ and $c_{ij} = 0$ when $i \neq j$. The next result gives a construction of circulant cyclotomic graphs.

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

Lemma 5.1. *Let $m \geq 2$ and $n \geq 3$ be odd integers, and let c_{ij} be defined by (16). Suppose that a is a positive integer such that*

$$a^i \equiv \sum_{j=0}^{\phi(m)-1} c_{ij} a^j \bmod n, \ \ \phi(m) \leq i \leq m-1 \tag{17}$$

and $a^m \equiv 1 \bmod n$ but $a^i \not\equiv \pm 1 \bmod n$ for $1 \leq i \leq m-1$. Then $\mathrm{Cay}(\mathbb{Z}_n, \langle [-a] \rangle) \cong G_m(A_{m,n,a})$, where

$$A_{m,n,a} := \left\{ \sum_{i=0}^{\phi(m)-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m] : \sum_{i=0}^{\phi(m)-1} a_i a^i \equiv 0 \bmod n \right\}. \tag{18}$$

Proof. Define

$$f\left(\sum_{i=0}^{\phi(m)-1} a_i \zeta_m^i \right) = \sum_{i=0}^{\phi(m)-1} a_i a^i \bmod n, \ \ a_i \in \mathbb{Z}. \tag{19}$$

Since $1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}$ is an integral basis for the $\mathbb{Z}$-module $\mathbb{Z}[\zeta_m]$, f is a well-defined mapping from $\mathbb{Z}[\zeta_m]$ to $\mathbb{Z}_n$. Obviously, f is surjective. Using (16)–(19), one can verify that $f\left(\sum_{i=0}^{k} a_i \zeta_m^i\right) = \sum_{i=0}^{k} a_i a^i$, $0 \leq k \leq n-1$. This can be easily extended to arbitrary k, that is, for any $k \geq 0$,

$$f\left(\sum_{i=0}^{k} a_i \zeta_m^i \right) = \sum_{i=0}^{k} a_i a^i \bmod n. \tag{20}$$

We claim that f is a ring homomorphism from $\mathbb{Z}[\zeta_m]$ to $\mathbb{Z}_n$. In fact, for $\alpha = \sum_{i=0}^{m-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$ and $\beta = \sum_{i=0}^{m-1} b_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$, it is evident that $f(\alpha+\beta) = f(\alpha) + f(\beta)$. Since $\zeta_m^m = 1$, we have

$$\alpha\beta = \sum_{k=0}^{m-1} \left(\sum_{i+j=k} a_i b_j \right) \zeta_m^k + \sum_{k=m}^{2(m-1)} \left(\sum_{i+j=k} a_i b_j \right) \zeta_m^{k-m}.$$

Thus, by (20) and the assumption $a^m \equiv 1 \bmod n$,

$$\begin{aligned} f(\alpha\beta) &= \sum_{k=0}^{m-1} \left(\sum_{i+j=k} a_i b_j \right) a^k + \sum_{k=m}^{2(m-1)} \left(\sum_{i+j=k} a_i b_j \right) a^{k-m} \bmod n \\ &= \left(\sum_{i=0}^{m-1} a_i a^i \right) \left(\sum_{i=0}^{m-1} b_i a^i \right) \bmod n \\ &= f(\alpha) f(\beta). \end{aligned}$$

Therefore, f is a surjective homomorphism from $\mathbb{Z}[\zeta_m]$ to $\mathbb{Z}_n$.

The kernel of f is exactly $A = A_{m,n,a}$ as defined in (18). By the homomorphism theorem for rings, we have $\mathbb{Z}[\zeta_m]/A \cong \mathbb{Z}_n$ and $\bar{f}(x+A) := f(x)$, $x \in \mathbb{Z}[\zeta_m]$ defines the corresponding isomorphism from $\mathbb{Z}[\zeta_m]/A$ to $\mathbb{Z}_n$. Since $f(\zeta_m^i) = a^i \bmod n$ by (20), $\bar{f}$ maps $\pm(\zeta_m^i + A)$ to $\pm[a^i]$, $0 \leq i \leq m-1$. Since m is odd, it follows that the subset E_m/A of $\mathbb{Z}[\zeta_m]/A$ defined in (1) with respect to A above is the pre-image of $\langle [-a] \rangle = \{\pm[a^i] : 0 \leq i \leq m-1\} \leq \mathbb{Z}_n^*$ under $\bar{f}$. Since n is odd and $a^m \equiv 1 \bmod n$, n is not a divisor of $2a^i$ for $0 \leq i \leq m-1$. This together with the assumption $a^i \not\equiv \pm 1 \bmod n$, $1 \leq i \leq m-1$ implies that $\langle [-a] \rangle$ has order $2m$. Therefore, E_m/A has size $2m$ and $\bar{f}$ gives a bijection from E_m/A to $\langle [-a] \rangle$. In

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

other words, $G_m(A)$ has valency $2m$. It is readily seen that $\bar{f}$ gives rise to an isomorphism from $G_m(A)$ to $\mathrm{Cay}(\mathbb{Z}_n, \langle[-a]\rangle)$. □

Lemma 5.2. *([33, Lemma 4]) Let $n \geq 3$ be an integer. A subgroup H of $\mathbb{Z}_n^*$ is semiregular on $\mathbb{Z}_n \setminus \{[0]\}$ if and only if $[h-1] \in \mathbb{Z}_n^*$ for all $[h] \in H \setminus \{[1]\}$.*

Theorem 5.3. *Let p be an odd prime and $n \geq 2p+1$ an integer. Then a $2p$-valent circulant $\mathrm{Cay}(\mathbb{Z}_n, S)$ with $[1] \in S$ is a first kind Frobenius graph with cyclic kernel if and only if $n \equiv 1 \bmod 2p$ and $S = \langle[a]\rangle$ for some positive integer a such that $a^p + 1 \equiv 0 \bmod n$ and $\gcd(a^i \pm 1, n) = 1$ for $1 \leq i \leq p-1$. Moreover, in this case $\mathrm{Cay}(\mathbb{Z}_n, \langle[a]\rangle)$ is a $\mathbb{Z}_n \rtimes \langle[a]\rangle$-arc transitive first kind $\mathbb{Z}_n \rtimes \langle[a]\rangle$-Frobenius circulant.*

Proof. Let $\mathrm{Cay}(\mathbb{Z}_n, S)$ be a first kind Frobenius circulant with order n such that $[1] \in S$ and the kernel of the underlying Frobenius group is $\mathbb{Z}_n$. Then there exists a subgroup H of $\mathbb{Z}_n^*$ such that $|H| = 2p$, $\mathbb{Z}_n \rtimes H$ is a Frobenius group and $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a first kind $\mathbb{Z}_n \rtimes H$-Frobenius circulant. Thus H is semiregular on $\mathbb{Z}_n \setminus \{[0]\}$, and in particular $n \equiv 1 \bmod 2p$. Moreover, S is an H-orbit on $\mathbb{Z}_n$ and hence H is regular on S. Since $[1] \in S$, it follows that $S = H$. Since H is Abelian with $|H| = 2p$, it is a cyclic group of order $2p$, as an Abelian group of order $2p$ must be cyclic. So we may assume $H = \langle[a]\rangle = \{[a^i] : 0 \leq i \leq 2p-1\}$, where $[a]$ is an element of $\mathbb{Z}_n^*$ with order $2p$. Since $[1] \in S$ and S is closed under taking negative elements, we have $-[1] \in S = H$ and so there exists i with $2 \leq i \leq 2p-1$ such that $[a^i] = -[1]$ (note that $[a] \neq -[1]$ as $[a]$ has order $2p > 2$ in $\mathbb{Z}_n^*$). Thus $[a^{2i}] = [1]$ and so $2p$ divides $2i$. Since p is a prime, we have $i = p$ and therefore $a^p + 1 \equiv 0 \bmod n$ (so that $H = \{\pm[1], \pm[a], \pm[a^2], \ldots, \pm[a^{p-1}]\}$). Since H is semiregular on $\mathbb{Z}_n \setminus \{[0]\}$, by Lemma 5.2, the integers $a^i \pm 1$ are all coprime to n for $1 \leq i \leq p-1$.

Conversely, if $n \equiv 1 \bmod 2p$ and a is a positive integer such that $a^p+1 \equiv 0 \bmod n$ and $a^i \pm 1$, $1 \leq i \leq p-1$ are coprime to n, then $H = \langle[a]\rangle \leq \mathbb{Z}_n^*$ is semiregular on $\mathbb{Z}_n \setminus \{[0]\}$ with order $|H| = 2p$. Therefore, $\mathbb{Z}_n \rtimes H$ is a Frobenius group and $\mathrm{Cay}(\mathbb{Z}_n, \langle[a]\rangle)$ is a first kind $\mathbb{Z}_n \rtimes H$-Frobenius graph. Moreover, $\mathrm{Cay}(\mathbb{Z}_n, \langle[a]\rangle)$ is $\mathbb{Z}_n \rtimes H$-arc-transitive by [40, Lemma 2.1]. □

Remark 5.4. Since $a^p+1 = (a+1)\sum_{i=0}^{p-1}(-1)^i a^i$ and $a^2-1 = (a-1)(a+1)$, the conditions in Theorem 5.3 are equivalent to that $a^{p-1} \equiv \sum_{i=0}^{p-2}(-1)^{i+1}a^i \bmod n$ and $\gcd(a^i \pm 1, n) = 1$ for $2 \leq i \leq p-1$. Thus each $[u] \in \mathbb{Z}_n$ can be expressed as $[u] = [\sum_{i=0}^{p-2} u_i a^i]$ for some integers $u_0, u_1, \ldots, u_{p-2}$. Obviously this representation is not unique and without loss of generality we may assume $u_i \geq 0$ for $0 \leq i \leq p-2$. The neighbours of $[u]$ are $[u] + [a^j]$, $0 \leq j \leq 2p-1$, and $H = \langle[a]\rangle$ cyclically 'rotates' the 'directions' $[a^j]$ at $[u]$ in the obvious way. From a geometric point of view this determines a cyclic permutation of the edges incident with $[u]$ and thus defines an embedding of $\mathrm{Cay}(\mathbb{Z}_n, \langle[a]\rangle)$ on a closed orientable surface as a balanced regular Cayley map (see [35, Corollary 2.9]). Note that $\mathrm{Cay}(\mathbb{Z}_n, \langle[a]\rangle)$ is a rotational Cayley graph.

Theorem 5.5. *Let p be an odd prime and $n \geq 2p+1$ an integer with $n \equiv 1 \bmod 2p$. Then the first kind Frobenius circulant $\mathrm{Cay}(\mathbb{Z}_n, \langle[a]\rangle)$ in Theorem 5.3 is isomorphic to $G_p(A_{p,n,-a})$.*

Proof. We have $\phi(p) = p-1$, $\zeta_p^{p-1} = -\sum_{j=0}^{p-2}\zeta_p^j$, and $A_{p,n,-a} = \{\sum_{i=0}^{p-2} a_i\zeta_p^i \in \mathbb{Z}[\zeta_p] : \sum_{i=0}^{p-2} a_i(-a)^i \equiv 0 \bmod n\}$. Since $a^p + 1 \equiv 0 \bmod n$ and $a+1$ is coprime to n, we have $(-a)^{p-1} \equiv -\sum_{j=0}^{p-2}(-a)^j \bmod n$, which means that $-a$ satisfies the condition (17). So $\mathrm{Cay}(\mathbb{Z}_n, \langle[a]\rangle) \cong G_p(A_{p,n,-a})$ by Lemma 5.1. □

Remark 5.6. In general, $A_{m,n,a}$ defined in (18) is not necessarily a principal ideal. However, it must be a principal ideal if m is one of the following integers:

$$3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$$

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

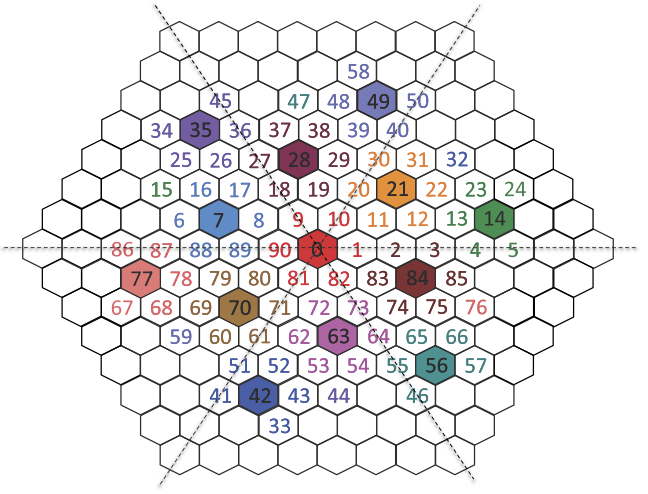

Fig. 1. A perfect 1-code in $EJ_{1+9\rho} \cong TL_{91}(10, 9, 1)$.

This is because there are precisely 29 cyclotomic fields $\mathbb{Q}(\zeta_m)$ with $\mathbb{Z}[\zeta_m]$ a principal ideal domain and they are given by these integers m [27]. Thus, by Theorem 5.5, we know that for $p = 3, 5, 7, 11, 13, 17, 19$, $\mathrm{Cay}(\mathbb{Z}_n, \langle [a] \rangle)$ in Theorem 5.3 is isomorphic to $G_p(\alpha)$ for some $0 \neq \alpha \in \mathbb{Z}[\zeta_p]$. It would be interesting to investigate when the converse of this statement is true (see [36, Theorem 5(b)] in the case when $p = 3$).

Problem 5.7. Let $t \geq 1$ be an integer. For $p = 5, 7, 11, 13, 17, 19$, find necessary and sufficient conditions for $(\beta)/(\alpha)$ to be a perfect t-code in $G_p(\alpha)$ (or $G_p^*(\alpha)$), where $0 \neq \alpha, \beta \in \mathbb{Z}[\zeta_p]$ such that β divides α.

In view of Corollary 4.3, the first key step towards this problem may be to acquire detailed knowledge of the distance in $G_p(\alpha)$ (or $G_p^*(\alpha)$) and the size of the t-neighbourhood of a vertex in the graph.

In the case when $p = 3$, Theorem 5.5 asserts that, for any odd integer $n \geq 7$ and positive integer a such that $a^2 - a + 1 \equiv 0 \bmod n$ and $a^2 \pm 1$ is coprime to n, the 6-valent first kind Frobenius circulant

$$TL_n(a, a-1, 1) := \mathrm{Cay}(\mathbb{Z}_n, \langle [a] \rangle)$$

is isomorphic to the Eisenstein–Jacobi graph $EJ_\alpha = G_3(A_{3,n,-a})$ (see Remark 3.3), a result noticed in [36, Theorem 5(a)] (with more details), where $A_{3,n,-a} = \{c + d\rho \in \mathbb{Z}[\rho] : c + da \equiv 0 \bmod n\} = (\alpha)$ for some $0 \neq \alpha \in \mathbb{Z}[\rho]$ as $\mathbb{Z}[\rho]$ is an Euclidean domain.

We finish this paper by the following example to illustrate Theorems 4.7 and 5.5.

Example 5.8. Let $a = 10$ and $n = a^2 - a + 1 = 91$. Then by Theorem 5.5 (see also [36, Example 2]) $TL_{91}(10, 9, 1)$ is isomorphic to EJ_α for some $0 \neq \alpha \in \mathbb{Z}[\rho]$. In fact, by [36, Theorem 5(a)], $\alpha = 1 + 9\rho$ and $f : x + 10y \bmod 91 \mapsto x + y\rho \bmod \alpha$ is an isomorphism from $TL_{91}(10, 9, 1)$ to $EJ_{1+9\rho}$, where x and y are integers. By Theorem 4.7, the only perfect t-codes in $EJ_{1+9\rho}$ of the form $(\beta)/(1 + 9\rho)$ are given by $\beta = (t + 1) + t\rho$, $t + (t + 1)\rho$ with β dividing $1 + 9\rho$, where $1 \leq t \leq 4$. One can see that, for $t = 2, 3, 4$, $N(\beta)$ is not a divisor of $N(1 + 9\rho) = 91$ and so β does not divide $1 + 9\rho$. Moreover, $1 + 2\rho$ does not divide $1 + 9\rho$ whilst $1 + 9\rho = (2 + \rho)(4 - \rho)$. Therefore, the only perfect code in $EJ_{1+9\rho}$ of the form $(\beta)/(1 + 9\rho)$ is $(2 + \rho)/(1 + 9\rho)$, which is a perfect 1-code with size $N(1 + 9\rho)/N(2 + \rho) = 13$.

It can be verified that $(2 + \rho)/(1 + 9\rho) = \{j(1 + 2\rho) \bmod (1 + 9\rho) : 0 \leq j \leq 12\}$. Since $f^{-1} : j(1 + 2\rho) \bmod (1 + 9\rho) \mapsto 21j \bmod 91$, $0 \leq j \leq 12$, we may view $(2 + \rho)/(1 + 9\rho)$ as the perfect 1-code $C := \{0, 21, 42, 63, 84, 14, 35, 56, 77, 7, 28, 49, 70\} \pmod{91}$ in $TL_{91}(10, 9, 1)$. Following [36, Section 5], we can represent this graph by its minimum distance diagram as shown in Fig. 1 (the area with numbers),

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

where each vertex is adjacent to the six vertices in the neighbouring cells. By the discussion in [36, Section 5], the whole plane can be tessellated by copies of this minimum distance diagram. The 13 coloured vertices (numbers) in Fig. 1 constitute the perfect 1-code C, and the ball of radius one centred at each coloured vertex consists of the coloured vertex itself and its six neighbours. For example, the ball of radius one centred at 84 is $\{84, 3, 2, 83, 74, 75, 85\}$, and that centred at 42 is $\{42, 52, 51, 41, 32, 33, 43\}$. Equivalently, we can label the hexagonal cells by the elements of $\mathbb{Z}[\rho]/(1 + 9\rho)$, say, $21 = 1 + 2 \cdot 10$ can be replaced by $1 + 2\rho$, $78 = 8 + 7 \cdot 10$ by $8 + 7\rho$, and so on.

Acknowledgements

The author was supported by the Australian Research Council (FT110100629). He thanks Alex Ghitza for helpful discussions on number theory and He Huang for critical comments on earlier versions of this paper.

References

[1] E. Bannai, On perfect codes in the Hamming schemes $H(n, q)$ with q arbitrary, J. Comb. Theory A 23 (1977) 52–67.
[2] J.-C. Bermond, F. Comellas, D.F. Hsu, Distributed loop computer networks: a survey, J. Parallel Distrib. Comput. 24 (1995) 2–10.
[3] N. Biggs, Perfect codes in graphs, J. Comb. Theory B 15 (1973) 289–296.
[4] I. Dejter, O. Serra, Efficient dominating sets in Cayley graphs, Discrete Appl. Math. 129 (2003) 319–328.
[5] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. 10 (1973) 1–97.
[6] Y-P. Deng, Y-Q. Sun, Q. Liu, H.-C. Wang, Efficient dominating sets in circulant graphs, Discrete Math. 340 (2017) 1503–1507.
[7] J.D. Dixon, B. Mortimer, Permutation Groups, Springer, New York, 1996.
[8] G. Etienne, Perfect codes and regular partitions in graphs and groups, Eur. J. Comb. 8 (2) (1987) 139–144.
[9] T. Etzion, On the nonexistence of perfect codes in the Johnson scheme, SIAM J. Discrete Math. 9 (1996) 201–209.
[10] Y. Fan, Y. Gao, Codes over algebraic integer rings of cyclotomic fields, IEEE Trans. Inf. Theory 50 (2004) 194–200.
[11] X.G. Fang, C.H. Li, C.E. Praeger, On orbital regular graphs and Frobenius graphs, Discrete Math. 182 (1998) 85–99.
[12] R. Feng, H. Huang, S. Zhou, Perfect codes in circulant graphs, Discrete Math. 340 (2017) 1522–1527.
[13] M. Flahive, B. Bose, The topology of Gaussian and Eisenstein–Jacobi interconnection networks, IEEE Trans. Parallel Distrib. Syst. 21 (2010) 1132–1142.
[14] O. Heden, A survey of perfect codes, Adv. Math. Commun. 2 (2008) 223–247.
[15] M.-C. Heydemann, N. Marlin, S. Pérenes, Complete rotations in Cayley graphs, Eur. J. Comb. 22 (2001) 179–196.
[16] M.-C. Heydemann, J.-C. Meyer, D. Sotteau, On forwarding indices of networks, Discrete Appl. Math. 23 (1989) 103–123.
[17] H. Huang, B. Xia, S. Zhou, Perfect codes in Cayley graphs, SIAM J. Discrete Math. 32 (2018) 548–559.
[18] K. Huber, Codes over Gaussian integers, IEEE Trans. Inf. Theory 40 (1994) 207–216.
[19] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Springer-Verlag, New York, 1990.
[20] R. Jajcay, J. Širáň, Skew-morphism of regular Cayley maps, Discrete Math. 244 (2002) 167–179.
[21] J. Kratochvíl, Perfect codes over graphs, J. Comb. Theory B 40 (1986) 224–228.
[22] J. Lee, Independent perfect domination sets in Cayley graphs, J. Graph Theory 37 (2001) 213–219.
[23] C. Martínez, R. Beivide, C. Camarero, E. Stafford, E.M. Gabidulin, Quotients of Gaussian graphs and their application to perfect codes, J. Symb. Comput. 45 (2010) 813–824.
[24] C. Martínez, R. Beivide, E. Gabidulin, Perfect codes for metrics induced by circulant graphs, IEEE Trans. Inf. Theory 53 (2007) 3042–3052.
[25] C. Martínez, R. Beivide, E. Gabidulin, Perfect codes from Cayley graphs over Lipschitz integers, IEEE Trans. Inf. Theory 55 (8) (2009) 3552–3562.
[26] C. Martínez, R. Beivide, E. Stafford, M. Moretó, E.M. Gabidulin, Modeling toroidal networks with the Gaussian integers, IEEE Trans. Comput. 57 (8) (2008) 1046–1056.
[27] J.M. Masley, H.L. Montgomery, Cyclotomic fields with unique factorization, J. Reine Angew. Math. 286/287 (1976) 248–256.
[28] N. Obradović, J. Peters, G. Ružić, Efficient domination in circulant graphs with two chord lengths, Inf. Process. Lett. 102 (6) (2007) 253–258.
[29] K. Reji Kumar, G. MacGillivray, Efficient domination in circulant graphs, Discrete Math. 313 (6) (2013) 767–771.
[30] M. Škoviera, J. Širáň, Regular maps from Cayley graphs, Part I: balanced Cayley maps, Discrete Math. 109 (1992) 265–276.
[31] P. Solé, The edge-forwarding index of orbital regular graphs, Discrete Math. 130 (1994) 171–176.
[32] S. Terada, Perfect codes in $\mathrm{SL}(2, 2^f)$, Eur. J. Comb. 25 (7) (2004) 1077–1085.
[33] A. Thomson, S. Zhou, Frobenius circulant graphs of valency four, J. Aust. Math. Soc. 85 (2008) 269–282.
[34] A. Thomson, S. Zhou, Gossiping and routing in undirected triple-loop networks, Networks 55 (2010) 341–349.
[35] A. Thomson, S. Zhou, Rotational circulant graphs, Discrete Appl. Math. 162 (2014) 296–305.

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007

[36] A. Thomson, S. Zhou, Frobenius circulant graphs of valency six, Eisenstein–Jacobi networks, and hexagonal meshes, Eur. J. Comb. 38 (2014) 61–78.
[37] J.H. van Lint, A survey of perfect codes, Rocky Mt. J. Math. 5 (1975) 199–224.
[38] L.C. Washington, Introduction to Cyclotomic Fields, 2nd ed., Springer, New York, 1997.
[39] J. Žerovnik, Perfect codes in direct products of cycles – a complete characterization, Adv. Appl. Math. 41 (2008) 197–205.
[40] S. Zhou, A class of arc-transitive Cayley graphs as models for interconnection networks, SIAM J. Discrete Math. 23 (2009) 694–714.
[41] S. Zhou, On 4-valent Frobenius circulant graphs, Discrete Math. Theor. Comput. Sci. 14 (2) (2012) 173–188.

Please cite this article in press as: S. Zhou, Cyclotomic graphs and perfect codes, J. Pure Appl. Algebra (2018), https://doi.org/10.1016/j.jpaa.2018.05.007