Commun. Combin., Cryptogr. & Computer Sci., 2 (2023), 127–131

ISSN:2783-5456
Communications in Combinatorics, Cryptography & Computer Science
Journal Homepage: http://cccs.sgh.ac.ir

On a Class of Symplectic Graphs and Their Automorphisms

Bahman Askari[a,*], Fataneh Karimi[b]

[a]Department of Mathematics, Qorveh Branch, Islamic Azad University, Qorveh, Iran.
[b]Department of Mathematics, Shahre' Kord Branch, Islamic Azad University, Shahre' Kord, Iran.

Abstract

It easy to see that each graph is a modification of a reduced graph Γ of the same rank. It is proved that for every reduced graph with binary rank $2r$, there is a unique maximal graph with binary rank $2r$ which conatins Γ as an induced subgraph. These maximal graphs are called symplectic graphs. In this paper, we study the symplectic graphs which are defined over a ring. We also find the automorphism group of symplectic graphs which are defined over $\mathbb{Z}_{p^n}$, where p is a prime number and n is positive integer.

Keywords: Automorphism, Symplectic Graph, Symplectic Group, Generalized Symplectic Graph.

2020 MSC: 05E18, 05C25.

1. Introduction

In this paper, a graph $\Gamma = \Gamma(\mathcal{V}, E)$ is considered as a simple undirected graph with vertex-set $V(\Gamma) = \mathcal{V}$, and edge-set $E(\Gamma) = E$.

In this paper, let R be a commutative ring with identity element 1, and let V be a free R - module of R - dimension $n \geqslant 2$. The symplectic form β is a bilinear form $\beta : V \times V \longrightarrow R$, such that $\beta(x, x) = 0$ for all $x \in V$. The pair (V, β) is called a symplectic space. The symplectic form $\beta : V \times V \longrightarrow R$ is called nonsingular, when the R-module homomorphism from V to $V^* = \mathrm{Hom}_R(V, R)$ given by $x \longmapsto \beta(\ , x)$ is an isomorphism, for all $x \in V$. In the sequence, assume that β is a nonsingular symplectic form.

Recall that an element x in V is unimodular if there is an $f \in V^*$ such that $f(x) = 1$. For $x \in V$, we call Rx a line. A hyperbolic pair$\{x, y\}$ is a pair of unimodular vectors in V with the property that $\beta(x, y) = 1$. The module $H = Rx \bigoplus Ry$ is called a hyperbolic plane.

Any unimodular vector $u \in V$ may be complemented to a hyperbolic pair as follow:
Since u is unimodular, there is an $f \in V^*$ with $f(u) = 1$. Since β is nonsingular, there is an v in V with $1 = f(u) = \beta(u, v)$. Then, $\{u, v\}$ is a hyperbolic pair. A ring R is stably free whenever $V = V_1 \oplus P$, V and V_1 are free R - modules, then P is a free R - module.

Proposition 1.1. [2] *Suppose that R is a stably free ring, and V be a symplectic space over R. Then V is an orthogonal direct sum $V = H_1 \perp H_2 \perp \ldots \perp H_m$ of hyperbolic planes $H_1, H_2, \ldots, H_m$. In particular, the dimension of V is even.*

*Corresponding author
Email addresses: dr.askari.b@gmail.com (Bahman Askari), fatanehkarimi1367@gmail.com (Fataneh Karimi)

Received: November 3, 2023 Revised: November 10, 2023 Accepted: November 19, 2023

Lemma 1.2. *[4] Let x and y be unimodular elements in V. Then $Rx = Ry$ if and only if $x = \lambda y$ for some $\lambda \in R^*$.*

Let $\Gamma(\mathcal{V}, E)$ and $\Lambda(\mathcal{V}', E')$ be two graphs. The mapping $\alpha : \mathcal{V} \longrightarrow \mathcal{V}'$ is a homomorphism from Γ to Λ if $v, w \in V(\Gamma)$ are adjacent in Γ, then $\alpha(v), \alpha(w) \in V'(\Lambda)$ are adjacent in Λ. An isomorphism between Γ and Λ is a bijection homomorphism $\alpha : \mathcal{V} \longleftrightarrow \mathcal{V}'$ with $v, w \in V(\Gamma)$ are adjacent in Γ, if and only if $\alpha(v), \alpha(w) \in \mathcal{V}'(\Lambda)$ are adjacent in Λ.
An automorphism of a graph Γ is an isomorphism from Γ to itself. The set of all automorphisms of Γ, with composition of functions, is called the automorphism group of Γ and denoted by $Aut(\Gamma)$.

In most situations, it is difficult to determine the automorphism group of a graph, but there are various in the literature and some of the recent works come in the references [3, 5]. Now, let Γ be a graph with automorphism group $G = Aut(\Gamma)$. For vertex $v \in V(\Gamma)$, let G_v denote the stabilizer subgroup of vertex v; that is, the subgroup of G containing of those automorphism that fix v. From first isomorphism theorem, we know that:

$$[G : G_v] = \frac{|G|}{|G_v|} \leqslant |V(\Gamma)|.$$

The graph Γ is called vertex-transitive if $G = Aut(\Gamma)$ acts transitively on $\mathcal{V} = V(\Gamma)$. In other words, for any two vertices $v, w \in V(\Gamma)$ there is an automorphism $\alpha \in Aut(\Gamma)$ such that $\alpha(v) = w$. Now if Γ is a vertex-transitive graph, then for each vertex $v \in V(\Gamma)$, we have

$$\frac{|G|}{|G_v|} = |\mathcal{V}| \Longrightarrow |G| = |G_v||\mathcal{V}|.$$

Let $\Gamma = (\mathcal{V}, E)$ be a graph. The action of $Aut(\Gamma)$ on $V(\Gamma)$ induces an action on $E(\Gamma)$, by the rule $\beta\{x, y\} = \{\beta(x), \beta(y)\}$, where $\beta \in Aut(\Gamma)$, and $\{x, y\} \in E(\Gamma)$. Γ is called edge transitive if this action is transitive.

2. symplectic and generalized symplectic group

Suppose that (V, β) and (V', β') are two symplectic spaces. An isometry from (V, β) to (V', β') is an R - isomorphism $\sigma : V \longrightarrow V'$ such that:

$$\beta(x_1, x_2) = \beta'(\sigma(x_1), \sigma(x_2)) \text{ for every elements } x_1, x_2 \in V.$$

It is easy to verify that the set of all isometries from (V, β) to (V, β) is a group; this group is called symplectic group over V and denoted by $SP_R(V)$.

Definition 2.1. Let $B = \{v_1, \dots, v_{2n}\}$ be a basis for the symplectic space (V, β). The matrix $B = (b_{ij})_{1 \leqslant i,j \leqslant 2n}$, where $b_{ij} = \beta(v_i, v_j)$ is called the matrix of the form β over B.

The following theorem has been obtained from the definition of symplectic space and has an easy proof.

Theorem 2.2. *Let (V, β) and (W, β') be two symplectic spaces with $\dim V = \dim W = 2n$. Suppose that B_1 and B_2 are ordered basis of V and W respectively. If we denote the matrices of β and β' with respects to the above basis by B and C respectively, then $T : V \longrightarrow W$ is an isometry from V to W if and only if $A^t CA = B$, where A is matrix of T with respect to B_1.*

Corollary 2.3. *Let R be a stably free ring and (V, β) be symplectic space over R. Then*

$$SP_R(V) = \{A | A \text{ is invertable and } A^t JA = J\}$$

where J is blockdiagonal matrix as follow:

$$J = \begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & -1 & 0 \end{pmatrix}$$

In [2] it is proved that, $Z(SP_R(V)) = \{\pm I_{2n}\}$, where $Z(SP_R(V))$ denotes the center of the group $SP_R(V)$. A commutative ring R have a stable range one if for all $\alpha, \beta \in R$ with $\langle \alpha, \beta \rangle = R$, there exist a δ in R such that $\alpha + \delta\beta \in R^*$.

Lemma 2.4. *[2] Let* R *be a commutative ring with stable range* 1 *and* $2 \in R$ *be an unit. Let* V *be a symplectic space over* R. *Then* $SP_R(V)$ *acts transitively on unimodular vectors and on hyperbolic planes.*

Definition 2.5. Generalized symplectic group over ring R is denoted by $GSP_R(V)$ and defined as follow:

$$GSP_R(V) = \{T | T \text{ is invertible over } R \text{ and } TJT^t = kJ \text{ for some } k \in R^*\}.$$

3. symplectic graphs

For all terminologies and notations not defined here, we follow [1, 2]. We now define a class of regular graphs, which is known as symplectic graphs.

Definition 3.1. Let (V, β) be a symplectic space over ring R. The symplectic graph over $SP_R(V)$ denoted by $\mathcal{G}SP_R(V)$, is a graph with vertex- set

$$\{Rx | x \text{ is unimodular in } V\},$$

and two vertices Rx and Ry are adjacent if and only if $\beta(x, y) \in R^*$.

This adjacency is well defined, since if x_1, x_2, y_1, y_2 are unimodular elements in V with $Rx_1 = Rx_2$ and $Ry_1 = Ry_2$, then there exist $\lambda, \mu \in R^*$ such that $x_1 = \lambda x_2$ and $y_1 = \mu y_2$. Therefore

$$\beta(x_1, y_1) \in R^* \iff \beta(\lambda x_2, \mu y_2) \in R^*$$
$$\iff \lambda\mu\beta(x_2, y_2) \in R^* \iff \beta(x_2, y_2) \in R^*.$$

Now from lemma 2.4 we have the following lemma that proved in [2].

Lemma 3.2. *Let* R *be a commutative ring with stable range* 1 *and* $2 \in R$ *be an unit. Then the symplectic graph* $\mathcal{G}SP_R(V)$ *is vertex-transitive and edge-transitive.*

We now define a symplectic graph over $R = \mathbb{Z}_{p^n}$. Let $V^{2\nu} \subseteq \mathbb{Z}_{p^n}^{(2\nu)}$ be a set of elements $(a_1, a_2, \ldots, a_{2\nu})$, where for all $1 \leqslant i \leqslant 2\nu$, $a_i \in \mathbb{Z}_{p^n}$ and there is an $i \in \{1, \ldots, 2\nu\}$ such that a_i is invertible in $\mathbb{Z}_{p^n}$. We define an equivalence relation $\sim_{p^n}$ on V by the following rule:

$$(a_1, a_2, \ldots, a_{2\nu}) \sim_{p^n} (b_1, b_2, \ldots, b_{2\nu}) \iff (a_1, a_2, \ldots, a_{2\nu}) = \lambda(b_1, b_2, \ldots, b_{2\nu}),$$

for some $\lambda \in \mathbb{Z}_{p^n}^*$.
Let $[a_1, \ldots, a_{2\nu}]$ denotes the equivalence class of $(a_1, \ldots, a_{2\nu})$ with respect to $\sim_{p^n}$, and let $V_{\sim_{p^n}}^{(2\nu)}$ be the set of all equivalence classes. We define the bilinear form $\beta : V_{\sim_{p^n}}^{(2\nu)} \times V_{\sim_{p^n}}^{(2\nu)} \longrightarrow R$ by the rule $\beta(x, y) = xJy^t$. The symplectic graph module p^n on $\mathbb{Z}_{p^n}^{(2\nu)}$, relative to J which is denoted by $SP_{p^n}^{(2\nu)}$, is a graph with vertex-set $\{[a_1, \ldots, a_{2\nu}] | (a_1, \ldots, a_{2\nu}) \in V^{(2\nu)}\}$ and adjacency defined by

$$[a_1, \ldots, a_{2\nu}] \text{ adjacent to } [b_1, \ldots, b_{2\nu}] \text{ if and only if } \beta(x, y) \in \mathbb{Z}_{p^n}^*,$$

where $x = (a_1, \ldots, a_{2\nu})$ and $y = (b_1, \ldots, b_{2\nu})$. In [4], it is proves that $SP_{p^n}^{(2\nu)}$ is a vertex and edge-transitive graph.
In the first step, note that β is a symplectic form over $\mathbb{Z}_{p^n}^{(2\nu)}$.

Lemma 3.3. *Each element of* $V := V_{\sim p^n}^{(2\nu)}$ *is unimodular.*

Proof. If we define $q : V \longrightarrow V^*$ by $q(x) = q_x$ where $q_x(v) = \beta(x, v)$, then q is an isomorphism. For $x = (a_1, \ldots, a_{2\nu})$, let a_i be invertible in $\mathbb{Z}_{p^n}$. If $i \geqslant \nu + 1$, then let $y = (0, \ldots, b_{i-\nu} = 1, 0, \ldots, 0)$ and so $\beta(x, y) = a_i b_{i-\nu} = 1$. If $i \leqslant \nu$, then let $y = (0, \ldots, b_{i+\nu} = 1, 0, \ldots, 0)$ and so $\beta(x, y) = a_i b_{i+\nu} = 1$. Then there is an $f = q_y \in V^*$ such that $q_y(x) = f(x) = 1$ and hence x is unimodular. □

By previous lemma, we conclude that for $R = \mathbb{Z}_{p^n}$, $\mathcal{GSP}_R(\nu)$ is isomorphic to $SP_{p^n}^{(2\nu)}$.
In [2], it is proved that $\mathbb{Z}_{p^n}$ has a stable range one, and we know that for $p \geqslant 2$, 2 is unit in $\mathbb{Z}_{p^n}$, where p is prime. Then by lemma 3.2. we conclude that $SP_{p^n}^{(2\nu)}$ is vertex-transitive and edge-transitive.

Lemma 3.4. *Let* p *be a prime integer and* $R = \mathbb{Z}_{p^n}$ *and* $V = \mathbb{Z}_{p^n}^{(2\nu)}$. *Suppose that* $T \in GSP_R(V)$. *We define* $\sigma_T : V \longrightarrow V$ *by the rule* $\sigma_T(x) = R(xT)$ *for all unimodular elements* $x \in V$. *Then* $T \in GSP_R(V)$ *if and only if* $\sigma_T \in Aut(\mathcal{GSP}_R(V))$.

Proof. Let $T \in GSP_R(V)$ and $R\alpha, R\beta \in SP_R(V)$, then for $T \in GSP_R(V)$ we have $TJT^t = kJ$, where $k \in \mathbb{Z}_{p^n}^*$. Then $\alpha J \beta^t = k^{-1} \alpha TJT^t \beta^t$ and $R\alpha$ is adjacent to $R\beta$ if and only if αT is adjancent to βT, hence $\sigma_T \in Aut(\mathcal{GSP}_R(V))$.
Conversely, assume that $\sigma_T \in Aut(\mathcal{GSP}_R(V))$, then

$$R\alpha \nsim R\beta \Longleftrightarrow \alpha J \beta^t \nsubseteq R^* \Longleftrightarrow \alpha J \beta^t = r,$$

for some $r \in \mathbb{Z}_{p^n} \setminus \mathbb{Z}_{p^n}^*$.
If $r = 0$, then $\alpha J \beta^t = 0$ if and only if $\alpha(TJT^t)\beta^t = 0$. Hence, for any nonzero $\alpha \in R$, two equations $(\alpha J)X^t = 0$ and $(\alpha TJT^t)X = 0$ have the same solutions. But $rank(\alpha J) = rank(\alpha TJT^t) = 1$, and so $\alpha k = s\alpha(TJT^t)$ for some $s \in R^*$.
Now let $\{e_1, \ldots, e_{2\nu}\}$ be the standard basis for V, then we obtine

$$J = diag(k_1, \ldots, k_{2\nu}) TJT^t,$$

for some $k_1, \ldots, k_{2\nu} \in R^{\times}$. If we put $\alpha = (1, \ldots, 1)$, then $k_1 = k_2 = \ldots = k_{2\nu} = k \in R^{\times}$, and so $J = KTJT^t$, $T \in GSP_R(V)$.
If $\alpha J \beta^t = r \neq 0$, then $r = P^n$ for $1 \leqslant m \leqslant n$, and $P^{n-m} \alpha J \beta^t = P^n = 0$, so we can do as above and then $T \in GSP_R(V)$.

□

We now proceed to proving the main result of this paper.

Theorem 3.5. *Let* $R = \mathbb{Z}_{p^n}$ *and* $V = \mathbb{Z}_{p^n}^{(2\nu)}$, *then*

$$Aut(\mathcal{GSP}_R(V)) = \frac{GSP_R(V)}{kI},$$

for some $k \in R^*$.

Proof. We define the homomorphism $\sigma : GSP_R(V) \longrightarrow Aut(\mathcal{GSP}_R(V))$ by $T \longmapsto \sigma_T$. In [5], it is proved that, $\sigma_{T_1} = \sigma_{T_2}$ if and only if $T_1 = kT_2$, for $k \in R^*$. Then $\ker \sigma = \{kI | \, k \in R^*\}$. Now it remains to show that for any $f \in Aut(\mathcal{GSP}_R(V))$, there is an $T \in GSP_R(V)$, such that $f = \sigma_T$. For any $\alpha \neq 0$ in V, we will denote $f(R\alpha \setminus \{0\})$ by $f(\alpha)$ and $f(0) = 0$. Since $f \in Aut(\mathcal{GSP}_R(V))$, then $\alpha J \beta^t = f(\alpha)J(f(\beta))^t$ for any $\alpha, \beta \in V$. Fix $\alpha \in V$ and let $\beta_1, \beta_2 \in V$, then $\alpha J \beta_1^t = f(\alpha)J(f(\beta_1))^t$ and $\alpha J \beta_2^t = f(\alpha)J(f(\beta_2))^t$ then $\alpha J(\beta_1 + \beta_2)^t = f(\alpha)J(f(\beta_1) + f(\beta_2))^t$. Thus, $\alpha J(\beta_1 + \beta_2)^t = f(\alpha)J(f(\beta_1 + \beta_2))^t$, hence $f(\alpha)J(f(\beta_1 + \beta_2) - f(\beta_1) - f(\beta_2)) = 0$ and therefor for all $\alpha \in V$, we have $f(\beta_1 + \beta_2) = f(\beta_1) + f(\beta_2)$. Let,

$$T = \begin{pmatrix} f(1,0,\dots,0) \\ f(0,1,\dots,0) \\ \vdots \\ f(0,0,\dots,1) \end{pmatrix}$$

Therefor $f(\alpha) = \alpha T$, for any $\alpha \in V$. Then T is nonsingular, so by lemma 3.4. $T \in SP_R(V)$ and $f = \sigma_T$.

□

References

[1] C. Godsil, G. Royal, *Algebric graph theory*, Speringer-Verlage New york (2001). 3

[2] B. Kirkwood, B.R. Mcdonald, R. P. Agarwal, *The symplectic group over a ring with one in its stable range*, Pacificy. Math., **92(1)**, (1981), 111–125. 1.1, 2, 2.4, 3, 3, 3

[3] Z. Liwei, C. Zhao, F. Rogcuan, M. Chagli, *Full automorphism group of generalized symplectic graph*, Sci. China Math, **56(7)**, (2013) 1509-1520. 1

[4] Y. Meemark, T. Prinyasart, *On symplectic graphs modulo* P^n, Discrete Math, **311(17)**, (2011) 1874–1878. 1.2, 3

[5] Z. Tang, Z. X. Wan, *Symplectic graphs and their automorphisms*, European J. Combin, **27(1)**, (2006) 38–50. 1, 3