J Algebr Comb (2011) 34:323–335
DOI 10.1007/s10801-011-0273-9

Elementary abelian p-groups of rank $2p+3$ are not CI-groups

Gábor Somlai

Received: 7 December 2009 / Accepted: 6 January 2011 / Published online: 2 February 2011

Abstract For every prime $p>2$ we exhibit a Cayley graph on $\mathbb{Z}_p^{2p+3}$ which is not a CI-graph. This proves that an elementary abelian p-group of rank greater than or equal to $2p+3$ is not a CI-group. The proof is elementary and uses only multivariate polynomials and basic tools of linear algebra. Moreover, we apply our technique to give a uniform explanation for the recent works of Muzychuk and Spiga concerning the problem.

Keywords Cayley graph · CI-group · Elementary abelian p-group

1 Introduction

Let G be a finite group and S a subset of G. The Cayley graph $\mathrm{Cay}(G,S)$ is defined by having the vertex set G and g is adjacent to h if and only if $gh^{-1}\in S$. The set S is called the connection set of the Cayley graph $\mathrm{Cay}(G,S)$. A Cayley graph $\mathrm{Cay}(G,S)$ is undirected if and only if $S=S^{-1}$, where $S^{-1}=\{s^{-1}\in G\mid s\in S\}$. Every right multiplication via elements of G is an automorphism of $\mathrm{Cay}(G,S)$, so the automorphism group of every Cayley graph on G contains a regular subgroup isomorphic to G. Moreover, this property characterises the Cayley graphs on G.

It is clear that $\mathrm{Cay}(G,S)\cong\mathrm{Cay}(G,S^\sigma)$ for every $\sigma\in\mathrm{Aut}(G)$. A Cayley graph $\mathrm{Cay}(G,S)$ is said to be a CI-graph if, for each $T\subset G$, the Cayley graphs $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(G,T)$ are isomorphic if and only if there is an automorphism σ of G such that $S^\sigma=T$. Furthermore, a group G is called a CI-group if every Cayley graph on G is a CI-graph.

Research supported by the Hungarian Scientific Fund (OTKA), grant no. NK72523.

G. Somlai (✉)
Department of Algebra and Number Theory, Eötvös University, Budapest, Hungary
e-mail: zsomlei@gmail.com

For our discussion two previous results are relevant. It is easy to prove that if G is a CI-group, then every subgroup of G is a CI-group. Babai and Frankl proved in [1] that the Sylow subgroups of a CI-group can only be $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{27}$, the quaternion group of order 8 or an elementary abelian p-group. Also, they asked whether every elementary abelian p-group is a CI-group.

Hirasaka and Muzychuk proved in [3] that $\mathbb{Z}_p^4$ is a CI-group for every prime p and this was also proved by Morris [4]. On the other hand, Muzychuk [5] proved that an elementary abelian p-group of rank $2p-1+\binom{2p-1}{p}$ is not a CI-group and most recently as a strengthening of this result Spiga [7] showed that if $n \geq 4p-2$, then $\mathbb{Z}_p^n$ is not a CI-group. Spiga [8] also proved that $\mathbb{Z}_3^5$ is a CI-group but $\mathbb{Z}_3^8$ is not a CI-group. The problem of determining whether or not an elementary abelian group $\mathbb{Z}_p^n$ is a CI-group is solved if $p=2$ as the CI property holds for $\mathbb{Z}_2^5$, see [2], and a non-CI-graph for $\mathbb{Z}_2^6$ was constructed by Nowitz [6].

Further improving the upper bounds in [5] and [7], we prove the following.

Theorem 1 *For every prime $p>2$, the group $\mathbb{Z}_p^{2p+3}$ has a Cayley graph of valency $(2p+3)p^{p+1}$ which is not a CI-graph. Consequently, an elementary abelian p-group of rank greater than or equal to $2p+3$ is not a CI-group.*

We can formulate a similar theorem for undirected Cayley graphs.

Theorem 2 *For every prime $p>3$, the group $\mathbb{Z}_p^{2p+3}$ has an undirected Cayley graph which is not a CI-graph.*

The problem of finding undirected non-CI-graphs of elementary abelian 3-groups is still open.

The proof of Theorem 1 is elementary and uses only the definition of the CI property. We will construct two isomorphic Cayley graphs in Sect. 2. The connection sets in both graphs are the union of affine subspaces in $\mathbb{Z}_p^{2p+3}$ and the isomorphism between the Cayley graphs is given in terms of polynomials. Finally, the proof in Sect. 5 that our Cayley graphs are not CI-graphs uses only elementary tools of linear algebra. Section 6 is devoted to prove Theorem 2. In addition, in Sect. 7 we will indicate how the previous results of Muzychuk and Spiga can be obtained applying our technique.

2 The construction

Let $U \cong \mathbb{Z}_p^{p+1}$ and $V \cong \mathbb{Z}_p^{p+2}$, then the groups U and V can be regarded as vector spaces over the field $\mathbb{Z}_p$ with bases $\{e_1, e_2, \ldots, e_{p+1}\}$ and $\{f_0, f_1, \ldots, f_{p+1}\}$, respectively. We endow V with the natural bilinear form:

$$\left\langle \sum_{j=0}^{p+1} \alpha_j f_j, \sum_{j=0}^{p+1} \beta_j f_j \right\rangle = \sum_{j=0}^{p+1} \alpha_j \beta_j.$$

Let us define the following affine subspaces of $G = U \oplus V$:

$$A_i = e_i + \{v \in V \mid \langle v, f_0 + f_i\rangle = 0\}, \quad (i = 1, \dots, p+1),$$

$$B_i = \sum_{j\neq i} e_j + \left\{v \in V \,\middle|\, \left\langle v, f_i + \sum_{j=0}^{p+1} f_j \right\rangle = 0\right\}, \quad (i = 1, \dots, p+1),$$

$$C_0 = \sum_{i=1}^{p+1} e_i + \left\{v \in V \,\middle|\, \left\langle v, \sum_{j=0}^{p+1} f_j \right\rangle = 0\right\},$$

$$C_1 = \sum_{i=1}^{p+1} e_i + \left\{v \in V \,\middle|\, \left\langle v, \sum_{j=0}^{p+1} f_j \right\rangle = 1\right\}.$$

Now

$$S = \bigcup_{i=1}^{p+1} (A_i \cup B_i) \cup C_0 \quad \text{and} \quad T = \bigcup_{i=1}^{p+1} (A_i \cup B_i) \cup C_1 \tag{1}$$

will be the connection sets of two Cayley graphs defined on $G = U \oplus V$. Note that the sets S and T are the union of affine subspaces of G. Namely, S and T are the union of $2p + 3$ affine subspaces of dimension $p + 1$. Therefore, $|S| = |T| = (2p + 3)p^{p+1}$, as desired.

We are going to show in Sect. 4 that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ but we will also prove in Sect. 5 that there is no automorphism of G mapping S to T. Taken together, these two facts establish Theorem 1.

3 Preliminary facts

In this section we introduce some notation concerning polynomials and we establish certain equations over the field $\mathbb{Z}_p$. These will be used in the proof of the isomorphism between the two Cayley graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, T)$.

For a sequence of integers $\underline{n} := (n_1, \dots, n_{p+1})$ we denote $x^{\underline{n}} := x_1^{n_1} \cdots x_{p+1}^{n_{p+1}}$ and let $k(x^{\underline{n}}) = |\{i \mid n_i > 0\}|$ denote the number of variables occurring in $x^{\underline{n}}$. Let $\mathcal{M}$ be the set of monomials of degree p involving at least two variables and for each $i = 1, \dots, p+1$ we divide it into two subsets $\mathcal{M} = \mathcal{M}_i^0 \cup \mathcal{M}_i^+$, where $\mathcal{M}_i^0 = \{x^{\underline{n}} \mid n_i = 0\}$ and $\mathcal{M}_i^+ = \{x^{\underline{n}} \mid n_i > 0\}$. For a monomial $x^{\underline{n}} \in \mathcal{M}$ we define the number $c_{\underline{n}} = \frac{(p-1)!}{n_1! \cdots n_{p+1}!}$. An obvious consequence of the Multinomial Theorem is that $\frac{p!}{n_1! \cdots n_{p+1}!}$ is an integer. If $x^{\underline{n}} \in \mathcal{M}$, then $k(x^{\underline{n}}) \geq 2$ so p does not divide the denominator of $c_{\underline{n}}$ and hence $c_{\underline{n}}$ is an integer. Finally, for $\underline{\alpha} \in \mathbb{Z}_p^k$ and $f(\underline{x}) \in \mathbb{Z}_p[x_1, \dots, x_k]$ we denote

$$\Delta_{\underline{\alpha}} f(\underline{x}) = f(\underline{x} + \underline{\alpha}) - f(\underline{x}).$$

Lemma 1 *Let $s = \sum_{i=1}^{p+1} x_i$ and $s_i = s - x_i = \sum_{j\neq i} x_j$.*

The following two equations hold over $\mathbb{Z}[x_1, \dots, x_{p+1}]$.

(a)

$$s^p = \sum_{j=1}^{p+1} {x_j}^p + \sum_{x^{\underline{n}} \in \mathcal{M}} p c_{\underline{n}} x^{\underline{n}}.$$

(b)

$$s_i^p = \sum_{j \neq i} {x_j}^p + \sum_{x^{\underline{n}} \in \mathcal{M}_i^0} p c_{\underline{n}} x^{\underline{n}}.$$

Proof These identities are obvious. □

Define the following polynomials in $\mathbb{Z}_p[x_1, \ldots, x_{p+1}]$:

$$r_i = \sum_{x^{\underline{n}} \in \mathcal{M}_i^0} \left(1 - k\left(x^{\underline{n}}\right)\right) c_{\underline{n}} x^{\underline{n}} + \sum_{x^{\underline{n}} \in \mathcal{M}_i^+} \left(2 - k\left(x^{\underline{n}}\right)\right) c_{\underline{n}} x^{\underline{n}} \tag{2}$$

for $i = 1, \ldots, p+1$ and

$$r_0 = \sum_{x^{\underline{n}} \in \mathcal{M}} \left(k\left(x^{\underline{n}}\right) - 2\right) c_{\underline{n}} x^{\underline{n}}. \tag{3}$$

Lemma 2

$$\sum_{j=0}^{p+1} r_j = \frac{p s^p - \sum_{j=1}^{p+1} s_j^p}{p}. \tag{4}$$

The polynomial $\frac{p s^p - \sum_{j=1}^{p+1} s_j^p}{p}$ *is defined in* $\mathbb{Z}[x_1, \ldots, x_{p+1}]$, *while* (4) *holds over* $\mathbb{Z}_p$.

Proof

$$\begin{aligned}\sum_{j=0}^{p+1} r_j &= \sum_{x^{\underline{n}} \in \mathcal{M}} \left(\left(p + 1 - k\left(x^{\underline{n}}\right)\right)\left(1 - k\left(x^{\underline{n}}\right)\right) + \left(k\left(x^{\underline{n}}\right) - 1\right)\left(2 - k\left(x^{\underline{n}}\right)\right)\right) c_{\underline{n}} x^{\underline{n}} \\ &= (1 - p) \sum_{x^{\underline{n}} \in \mathcal{M}} \left(k\left(x^{\underline{n}}\right) - 1\right) c_{\underline{n}} x^{\underline{n}} = \sum_{x^{\underline{n}} \in \mathcal{M}} \left(k\left(x^{\underline{n}}\right) - 1\right) c_{\underline{n}} x^{\underline{n}} \end{aligned} \tag{5}$$

and Lemma 1 gives

$$\frac{p s^p - \sum_{j=1}^{p+1} s_j^p}{p} = \sum_{x^{\underline{n}} \in \mathcal{M}} \left(k\left(x^{\underline{n}}\right) - 1\right) c_{\underline{n}} x^{\underline{n}}$$

as well. □

4 Isomorphism

Proposition 1 $\mathrm{Cay}(G,S)\cong\mathrm{Cay}(G,T)$.

Proof Let $\phi:\mathbb{Z}_p^{2p+3}\to\mathbb{Z}_p^{2p+3}$ be defined by

$$\begin{aligned}&\phi(x_1,\dots,x_{p+1},y_0,y_1,\dots,y_{p+1})\\&\quad=\bigl(x_1,\dots,x_{p+1},y_0+r_0(x_1,\dots,x_{p+1}),\dots,y_{p+1}+r_{p+1}(x_1,\dots,x_{p+1})\bigr),\end{aligned}$$

where $r_i\in\mathbb{Z}_p[x_1,\dots,x_{p+1}]$ are defined by (2) and (3).

We claim that ϕ is an isomorphism from $\mathrm{Cay}(G,S)$ to $\mathrm{Cay}(G,T)$. Note that ϕ acts by translation on $u+V$ for every $u\in U$ so ϕ is bijective. It remains to show that for $a,b\in G$ if $b-a\in S$, then $\phi(b)-\phi(a)\in T$.

Since G is the direct sum of U and V, an element $u+v\in G$ can be written as $(\underline{x},\underline{y})$, where $\underline{x}\in U$ and $\underline{y}\in V$. We will also write $u+v\in G$ as $(x_1,\dots,x_{p+1},y_0,y_1,\dots,y_{p+1})$.

Assume first that $b-a\in A_i$ for some $1\le i\le p+1$ and write $a=(\underline{x},\underline{y})$ with $\underline{x}\in U$ and $\underline{y}\in V$. Then we may set $b=a+(e_i+v)$, where $v\in V$ such that $\langle v,f_0+f_i\rangle=0$. Clearly ϕ does not affect the first $p+1$ coordinates hence we need to show $\phi(b)-\phi(a)\in A_i$. Now we have

$$\begin{aligned}\bigl(\phi(b)-\phi(a)\bigr)-(b-a)&=\bigl(\phi(b)-b\bigr)-\bigl(\phi(a)-a\bigr)\\&=\bigl(0,\dots,0,\Delta_{e_i}r_0(\underline{x}),\Delta_{e_i}r_1(\underline{x}),\dots,\Delta_{e_i}r_{p+1}(\underline{x})\bigr).\end{aligned}$$

Thus we have to check that $\langle(\Delta_{e_i}r_0(\underline{x}),\Delta_{e_i}r_1(\underline{x}),\dots,\Delta_{e_i}r_{p+1}(\underline{x})),f_0+f_i\rangle=0$. Now

$$\begin{aligned}\bigl\langle\bigl(\Delta_{e_i}r_0(\underline{x}),\Delta_{e_i}r_1(\underline{x}),\dots,\Delta_{e_i}r_{p+1}(\underline{x})\bigr),f_0+f_i\bigr\rangle&=\Delta_{e_i}r_0(\underline{x})+\Delta_{e_i}r_i(\underline{x})\\&=\Delta_{e_i}\bigl(r_0(\underline{x})+r_i(\underline{x})\bigr)=0,\end{aligned}$$

since r_0+r_i does not involve x_i.

By the same argument if $b-a\in C_0$, then using Lemma 2 we get

$$\begin{aligned}\Delta_{\sum_{j=1}^{p+1}e_j}\left(\sum_{j=0}^{p+1}r_j\right)&=\frac{p(s+p+1)^p-\sum_{j=1}^{p+1}(s_j+p)^p}{p}-\frac{ps^p-\sum_{j=1}^{p+1}s_j^p}{p}\\&=(s+1)^p-s^p=1.\end{aligned}$$

These equations hold over $\mathbb{Z}_p$ since $(t+p)^p\equiv t^p\pmod{p^2}$. Hence if $b-a\in C_0$, then $\phi(b)-\phi(a)\in C_1$.

Finally, if $b-a\in B_i$ we need a little more computation. Equation (5) shows that

$$\sum_{j=0}^{p+1}r_j=\sum_{x^{\underline{n}}\in\mathcal{M}}\bigl(k\bigl(x^{\underline{n}}\bigr)-1\bigr)c_{\underline{n}}x^{\underline{n}}.$$

Hence

$$\begin{aligned} r_i + \sum_{j=0}^{p+1} r_j &= \sum_{x^{\underline{n}} \in \mathcal{M}_i^0} \bigl(1 - k\bigl(x^{\underline{n}}\bigr)\bigr) c_{\underline{n}} x^{\underline{n}} + \sum_{x^{\underline{n}} \in \mathcal{M}_i^+} \bigl(2 - k\bigl(x^{\underline{n}}\bigr)\bigr) c_{\underline{n}} x^{\underline{n}} \\ &\quad + \sum_{x^{\underline{n}} \in \mathcal{M}} \bigl(k\bigl(x^{\underline{n}}\bigr) - 1\bigr) c_{\underline{n}} x^{\underline{n}} \\ &= \sum_{x^{\underline{n}} \in \mathcal{M}_i^+} c_{\underline{n}} x^{\underline{n}}, \end{aligned}$$

which is, by Lemma 1, equal to

$$\frac{s^p - x_i^p - s_i^p}{p}.$$

Therefore,

$$\Delta_{\sum_{j \neq i} e_j} \left(r_i + \sum_{j=0}^{p+1} r_j \right) = \frac{(s+p)^p - x_i^p - (s_i + p)^p}{p} - \frac{s^p - x_i^p - s_i^p}{p} = 0,$$

using again the fact that $(t + p)^p \equiv t^p \pmod{p^2}$. Hence if $b - a \in B_i$, then $\phi(b) - \phi(a) \in B_i$ and this finishes the proof of the fact that ϕ is indeed a graph isomorphism. □

5 Checking the CI property

Now in order to show that $\mathrm{Cay}(G, S)$ is not a CI-graph we have to show that there is no $\sigma \in \mathrm{Aut}(G) = \mathrm{GL}(U \oplus V)$ such that $\sigma(S) = T$.

Proposition 2 *There is no linear transformation $\sigma \in \mathrm{GL}(U \oplus V)$ such that $\sigma(S) = T$.*

Proof Assume by way of contradiction that $\sigma \in \mathrm{GL}(U \oplus V)$ with $\sigma(S) = T$. Let M denote the matrix of the linear transformation σ with respect to the basis $\{e_1, \dots, e_{p+1}, f_0, f_1, \dots, f_{p+1}\}$ and write $M = \bigl[\begin{smallmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{smallmatrix}\bigr]$ as a block matrix, where $M_{1,1} \in \mathbb{Z}_p^{(p+1)\times(p+1)}$ and $M_{2,2} \in \mathbb{Z}_p^{(p+2)\times(p+2)}$.

For the purpose of the following we modify our notation as follows. Let $S = \bigcup_{i=1}^{2p+3} S_i$ and $T = \bigcup_{i=1}^{2p+3} T_i$, where $S_i = T_i = A_i$, $S_{i+p+1} = T_{i+p+1} = B_i$ for $i = 1, \dots, p+1$ and $S_{2p+3} = C_0$, $T_{2p+3} = C_1$.

Now we prove two lemmas from which the proof of Proposition 2 will follow.

Lemma 3 *V is an invariant subspace of σ, i.e., $M_{1,2} = 0$.*

Proof Considering only the first $p+1$ coordinates it is easy to see using the assumption $p>2$ that for $i \neq j$ if $a \in S_i$ and $b \in S_j$, then $2a-b \notin S$ and similarly for T. This implies that both S and T contain exactly $2p+3$ affine subspaces of dimension $p+1$. Hence for $1 \le i \le 2p+3$ we must have $\sigma(S_i)=T_j$ for some j and if a, $b \in S_i$, then $\sigma(a)-\sigma(b) \in V$. Now

$$\operatorname{Span}\left(\bigcup_{i=1}^{p+1}\{a-b \mid a,b \in S_i\}\right)=V,$$

so $\sigma(V) \subseteq V$ and this finishes the proof of the fact that V is an invariant subspace of σ. □

It is immediate from Lemma 3 that σ induces a linear transformation of $(U \oplus V)/V$, which we also denote by σ. Set

$$\hat{S}=\left\{e_i, \sum_{j\neq i} e_j \mid 1 \le i \le p+1\right\} \cup \left\{\sum_{j=1}^{p+1} e_j\right\} \subset U. \tag{6}$$

In the following, Lemma 4, we shall identify the elements in $\hat{S}+V \subset (U \oplus V)/V$ with those in $\hat{S}$. As $\sigma(S)=\sigma(T)$ and $S+V=T+V$, we have $\sigma(\hat{S})=\hat{S}$.

Lemma 4 *$M_{1,1}$ is a permutation matrix.*

Proof In this proof we will use the natural bilinear form on U defined as follows:

$$\left[\sum_{i=1}^{p+1}\alpha_i e_i, \sum_{i=1}^{p+1}\beta_i e_i\right]=\sum_{i=1}^{p+1}\alpha_i\beta_i.$$

Let $e:=\sum_{i=1}^{p+1} e_i$. Note that e is the unique element of $\hat{S}$ which is the sum of two others within $\hat{S}$, hence $\sigma(e)=e$. The rest of the points can be paired such that the sum of every pair is e and by the linearity of σ the set $H=\{\sigma(e_i) \mid 1 \le i \le p+1\}$ contains exactly one element of each pair. Furthermore, $\sum_{h\in H} h=\sum_{i=1}^{p+1}\sigma(e_i)=\sigma(\sum_{i=1}^{p+1} e_i)=\sigma(e)=e$.

For every $s \in \hat{S}$ we have $[s,e]=0$ or 1, hence if H contains an element x such that $[x,e]=0$, then H contains p elements with the same property as $[\sum_{h\in H} h, e]=[e,e]=1$. By permuting the coordinates we obtain that if H contains an element x such that $[x,e]=0$, then $H=\{e_1\} \cup \{\sum_{j\neq i} e_j \mid 2 \le i \le p+1\}$ but $\sum_{h \in H} h = e_1-e_2-\cdots-e_{p+1} \neq \sum_{i=1}^{p+1} e_i=e$ in this case, a contradiction. □

Now we continue the proof of Proposition 2.

For every permutation of $\{e_1,\dots,e_{p+1}\}$ if we apply the same permutation to the indices of $\{f_1,\dots,f_{p+1}\}$ and fix f_0 we obtain an automorphism of $\operatorname{Cay}(G,S)$. Hence we may assume for the rest of the proof that $M_{1,1}=I$.

This assumption implies that $\sigma(e_i) \in A_i$ and $\sigma(\sum_{j\neq i} e_j) \in B_i$ for $1 \le i \le p+1$. From this we get

$$\langle M_{2,1}e_i, f_0 + f_i\rangle = 0,$$
$$\left\langle M_{2,1}\sum_{j\neq i} e_j, f_i + \sum_{j=0}^{p+1} f_j\right\rangle = 0$$

for $1 \le i \le p+1$.

The sum of these $2p+2$ equations over $\mathbb{Z}_p$ is

$$\sum_{i=1}^{p+1}\langle M_{2,1}e_i, f_0 + f_i\rangle + \sum_{i=1}^{p+1}\left\langle M_{2,1}\sum_{j\neq i} e_j, f_i + \sum_{j=0}^{p+1} f_j\right\rangle = 0,$$

so using bilinearity

$$\left\langle M_{2,1}\sum_{i=1}^{p+1} e_i, \sum_{j=0}^{p+1} f_j\right\rangle = 0.$$

We also have $\sigma(\sum_{j=1}^{p+1} e_j) \in C_1$, which gives

$$\left\langle M_{2,1}\sum_{i=1}^{p+1} e_i, \sum_{j=0}^{p+1} f_j\right\rangle = 1.$$

This contradiction finishes the proof of Proposition 2. □

Finally, Proposition 1 and Proposition 2 prove Theorem 1.

6 Undirected graphs

In this section we study undirected Cayley graphs and we will prove Theorem 2.

If G is an abelian group we write $-S = \{-s \in G \mid s \in G\}$ instead of S^{-1}. For a subset S of G we define $\bar{S} = S \cup -S$. It is also clear that if ϕ is an isomorphism between $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, T)$, then ϕ is an isomorphism between $\mathrm{Cay}(G, \bar{S})$ and $\mathrm{Cay}(G, \bar{T})$ as well.

In Sect. 2 we defined two isomorphic directed Cayley graphs $\mathrm{Cay}(\mathbb{Z}_p^{2p+3}, S)$ and $\mathrm{Cay}(\mathbb{Z}_p^{2p+3}, T)$ of $\mathbb{Z}_p^{2p+3}$, where S and T were defined in (1). Therefore, we have a pair of isomorphic undirected Cayley graphs: $\mathrm{Cay}(\mathbb{Z}_p^{2p+3}, \bar{S})$ and $\mathrm{Cay}(\mathbb{Z}_p^{2p+3}, \bar{T})$.

Proposition 3 *For every prime $p > 3$, the graph $\mathrm{Cay}(\mathbb{Z}_p^{2p+3}, \bar{S})$ is an undirected Cayley graph on the group $\mathbb{Z}_p^{2p+3}$ which is not a CI-graph.*

Proof It is enough to show that there is no linear transformation σ such that $\sigma(\bar{S}) = \bar{T}$. Seeking a contradiction, let us assume that $\sigma \in \mathrm{GL}(U \oplus V)$ with $\sigma(\bar{S}) = \bar{T}$.

The same kind of reasoning as in Lemma 3 shows that V is an invariant subspace of σ, but here we have to use the extra condition that $p > 3$. Hence σ induces a linear transformation of $(U \oplus V)/V$, which we also denote by σ. Set

$$\tilde{S} = \left\{ e_i, -e_i, \sum_{j \neq i} e_j, -\sum_{j \neq i} e_j \,\middle|\, 1 \le i \le p+1 \right\} \cup \left\{ \sum_{j=1}^{p+1} e_j, -\sum_{j=1}^{p+1} e_j \right\},$$

which is a subset of U. We shall identify the elements in $\tilde{S} + V \subset (U \oplus V)/V$ with those in $\tilde{S}$. As $\sigma(\bar{S}) = \sigma(\bar{T})$ and $\bar{S} + V = \bar{T} + V$, we have $\sigma(\tilde{S}) = \tilde{S}$. Note that we can write $\tilde{S} = \hat{S} \cup -\hat{S}$ with $\hat{S} \cap -\hat{S} = \emptyset$, where $\hat{S}$ is defined in (6).

Now we prove a lemma from which the proof of Proposition 3 will follow.

Lemma 5 *One of the two linear transformations σ and $-\sigma$ permutes the elements of $\hat{S}$.*

Proof Since σ induces an automorphism of $\mathrm{Cay}(U, \tilde{S})$ and $\sigma(0) = 0$, it gives an automorphism of the induced subgraph on the neighbourhood of 0 as well. In this subgraph the vertices e and $-e$ have degree $2p+2$, the other vertices have degree 2. This implies that $\sigma(e) = e$ or $\sigma(e) = -e$. So either σ or $-\sigma$ fixes e. The neighbourhood of e in $\tilde{S}$ is $\hat{S}$, hence the proof of Lemma 4 yields the result. □

As a consequence of Lemma 5 we get a linear transformation (σ or $-\sigma$) which maps S onto T. This contradicts Proposition 2, finishing the proof of Theorem 2. □

7 Connection to previous results

In this section, we modify our construction a little bit to get non-CI-graphs of the groups $\mathbb{Z}_p^{4p-2}$ and $\mathbb{Z}_p^{2p-1+\binom{2p-1}{p}}$. These results provide a uniform explanation for the recent work of Spiga [7] and Muzychuk [5], respectively. The proof of these results only simplifies the heavy machinery used in [5] and [7].

7.1 Rank $4p-2$

Let $U' \cong V' \cong \mathbb{Z}_p^{2p-1}$ and $W' = U' \oplus V'$ with the bases $\{e_1', \dots, e_{2p-1}'\}$ and $\{f_1', \dots, f_{2p-1}'\}$, respectively. We denote by $\mathcal{L}$ the set of multilinear monomials of degree p in $2p-1$ variables. Let $\mathcal{L}_i^0 = \{x^{\underline{n}} \in \mathcal{L} \mid n_i = 0\}$ and $\mathcal{L}_i^+ = \mathcal{L} \setminus \mathcal{L}_i^0$. If $x^{\underline{n}} \in \mathcal{L}$, then the exponent vector $\underline{n}$ can be treated as a p-element subset of $\{1, \dots, 2p-1\}$.

Let

$$A_i' = e_i' + \{ v' \in V' \mid \langle v', f_i' \rangle = 0 \},$$

$$B'_i = \sum_{j\neq i} e'_j + \left\{ v' \in V' \middle| \left\langle v', f'_i + \sum_{j=1}^{2p-1} f'_j \right\rangle = 0 \right\},$$

$$C'_0 = \sum_{j=1}^{2p-1} e'_j + \left\{ v' \in V' \middle| \left\langle v', \sum_{j=1}^{2p-1} f'_j \right\rangle = 0 \right\},$$

$$C'_1 = \sum_{j=1}^{2p-1} e'_j + \left\{ v' \in V' \middle| \left\langle v', \sum_{j=1}^{2p-1} f'_j \right\rangle = -1 \right\}.$$

Similarly to the construction in Sect. 2 let $S' = \bigcup_{i=1}^{2p-1}(A'_i \cup B'_i) \cup C'_0$ and $T' = \bigcup_{i=1}^{2p-1}(A'_i \cup B'_i) \cup C'_1$. We claim that $\mathrm{Cay}(W', S') \cong \mathrm{Cay}(W', T')$ and the isomorphism is given in the same manner:

$$\begin{aligned}&\phi'(x_1, \ldots, x_{2p-1}, y_1, \ldots, y_{2p-1})\\&\quad = \bigl(x_1, \ldots, x_{2p-1}, y_1 + l_1(x_1, \ldots, x_{2p-1}), \ldots, y_{2p-1} + l_{2p-1}(x_1, \ldots, x_{2p-1})\bigr),\end{aligned}$$

where l_i denotes the sum of the monomials in $\mathcal{L}_i^0$ for $i = 1, \ldots, 2p-1$.

In this case the computations needed to show that ϕ' is an isomorphism of the two Cayley graphs are easier.

Lemma 6 *Assume that* $x^{\underline{n}} \in \mathcal{L}$ *and* $\underline{m} \in \{0,1\}^{2p-1} \subseteq U'$

(a)

$$\bigl(\Delta_{\underline{m}} x^{\underline{n}}\bigr)(\underline{x}) = x^{\underline{n}\setminus\underline{m}} \sum_{\underline{k} \subsetneq \underline{n}\cap\underline{m}} x^{\underline{k}}.$$

(b)

$$\bigl(\Delta_{\sum_{j=1} e'_j} x^{\underline{n}}\bigr)(\underline{x}) = \sum_{\underline{k} \subsetneq \underline{n}} x^{\underline{k}}.$$

Proof (a) is obvious and (b) is just a particular case of (a). □

The proof that ϕ' is an isomorphism is similar to the proof of Proposition 1. We leave it to the reader to prove, using Lemma 7(a), that if $b - a \in A'_i$, then $\phi'(b) - \phi'(a) \in A'_i$, to prove, using Lemma 7(c), that if $b - a \in B'_i$, then $\phi'(b) - \phi'(a) \in B'_i$, and finally to prove, using Lemma 7(b), that if $b - a \in C'_0$, then $\phi'(b) - \phi'(a) \in C'_1$.

Lemma 7

(a)

$$\Delta_{e'_i} l_i = 0.$$

(b)

$$\Delta_{\sum_{j=1}^{2p-1} e'_j}\left(\sum_{j=1}^{2p-1} l_j\right) = -1.$$

(c)

$$\Delta_{\sum_{j\neq i} e'_j}\left(l_i + \sum_{j=0}^{2p-1} l_j\right) = 0.$$

Proof (a) Obvious, since l_i does not involve x_i.

(b) We have

$$\sum_{j=1}^{2p-1} l_j = \sum_{j=1}^{2p-1} \sum_{x^{\underline{n}}\in\mathcal{L}_i^0} x^{\underline{n}} = \sum_{x^{\underline{n}}\in\mathcal{L}} (p-1)x^{\underline{n}} = -\sum_{x^{\underline{n}}\in\mathcal{L}} x^{\underline{n}} \tag{7}$$

and hence

$$\Delta_{\sum_{j=1}^{2p-1} e'_j}\left(\sum_{j=1}^{2p-1} l_j\right) = -\Delta_{\sum_{j=1}^{2p-1} e'_j} \sum_{x^{\underline{n}}\in\mathcal{L}} x^{\underline{n}} = -\sum_{x^{\underline{n}}\in\mathcal{L}} \Delta_{\sum_{j=1}^{2p-1} e'_j} x^{\underline{n}}$$

applying Lemma 6(b)

$$\begin{aligned} &= -\sum_{\substack{\underline{n}\in\{0,1\}^{2p-1}\\ |\underline{n}|=p}} \sum_{\underline{k}\subsetneq\underline{n}} x^{\underline{k}} = -\sum_{|\underline{k}|<p} x^{\underline{k}} \sum_{\substack{\underline{k}\subseteq\underline{n}\\ |\underline{n}|=p}} 1 \\ &= -\sum_{|\underline{k}|<p} \binom{2p-1-|\underline{k}|}{p-|\underline{k}|} x^{\underline{k}}. \end{aligned}$$

The binomial coefficient $\binom{2p-1-|\underline{k}|}{p-|\underline{k}|}$ is divisible by p if $1 \le |\underline{k}| < p$ and this implies that the remaining polynomial is just the constant polynomial $-\binom{2p-1}{p}$ over $\mathbb{Z}_p$. Taking into account that $\binom{2p-1}{p} \equiv 1 \pmod{p}$, we obtain (b).

(c) Making use of (7) we get

$$l_i + \sum_{j=1}^{2p-1} l_j = \sum_{x^{\underline{n}}\in\mathcal{L}_i^0} x^{\underline{n}} - \sum_{x^{\underline{n}}\in\mathcal{L}} x^{\underline{n}} = -\sum_{x^{\underline{n}}\in\mathcal{L}_i^+} x^{\underline{n}}.$$

Now

$$\Delta_{\sum_{j\neq i} e'_j}\left(-\sum_{x^{\underline{n}}\in\mathcal{L}_i^+} x^{\underline{n}}\right) = -\sum_{x^{\underline{n}}\in\mathcal{L}_i^+} \Delta_{\sum_{j\neq i} e'_j} x^{\underline{n}}$$

and by Lemma 6(a)

$$= -\sum_{x^{\underline{n}}\in\mathcal{L}_i^+} x_i \sum_{\underline{k}\subsetneq\underline{n}\setminus\{i\}} x^{\underline{k}} = -x_i \sum_{\substack{i\notin\underline{k}\\ |\underline{k}|<p-1}} x^{\underline{k}} \sum_{\substack{\{i\}\cup\underline{k}\subsetneq\underline{n}\\ |\underline{n}|=p}} 1$$

$$= -x_i \sum_{\substack{i\notin\underline{k}\\ |\underline{k}|<p-1}} \binom{2p-1-|\underline{k}|-1}{p-|\underline{k}|-1} x^{\underline{k}}.$$

Now if $|k| < p-1$, then $\binom{2p-1-|\underline{k}|-1}{p-|\underline{k}|-1} \equiv 0 \pmod{p}$ and this proves the result. □

The proof of the fact that there is no linear transformation which maps S' to T' is nearly the same as in Proposition 2 provided $p > 3$. We leave it to the reader to work out the details and we will do so in the next case as well. If $p = 3$, then the statement analogous to Lemma 4 does not hold.

7.2 Rank $2p - 1 + \binom{2p-1}{p}$

Here we only give the connection sets and the isomorphism of the Cayley graphs. The proof goes along the same lines as in the previous cases.

Let $\mathcal{O} = \{\underline{k} \subset \{1, \dots, 2p-1\} \mid |\underline{k}| = p\}$ and let $U'' \cong \mathbb{Z}_p^{2p-1}$ and $V'' \cong \mathbb{Z}_p^{\binom{2p-1}{p}}$ with the bases $\{e_1'', e_2'', \dots, e_{2p-1}''\}$ and $\{f_{\underline{k}}'' \mid \underline{k} \in \mathcal{O}\}$, respectively. Since $|\mathcal{O}|$ equals to the dimension of V'', for every $\underline{y''} \in V''$ we can write $\underline{y''} = (\dots, y_{\underline{k}}'', \dots)$, where $\underline{k} \in \mathcal{O}$. For $(\underline{x''}, \underline{y''}) \in U'' \oplus V''$ we define

$$\phi''(\underline{x}'', \underline{y}'') = \bigl(\underline{x}'', \dots, y_{\underline{k}}'' + x''^{\underline{k}}, \dots\bigr).$$

For each $1 \le i \le 2p-1$ we define the set

$$A_i'' = e_i'' + \left\{ v'' \in V'' \,\middle|\, \left\langle v'', \sum_{i\notin\underline{k}} f_{\underline{k}}'' \right\rangle = 0 \right\}.$$

For every $\underline{k} \in \mathcal{O}$ there are exactly p elements $\underline{k}_1, \dots, \underline{k}_p$ of $\mathcal{O}$ such that $|\underline{k} \cap \underline{k}_i| = 1$ and hence we can define

$$B_{\underline{k}}'' = \sum_{j\in\underline{k}} e_j'' + \bigl\{ v'' \in V'' \big| \langle v'', f_{\underline{k}_1}'' + \dots + f_{\underline{k}_p}'' \rangle = 0 \bigr\}.$$

The third type of affine subspaces are defined by

$$C_0'' = \sum_{j=1}^{2p-1} e_j'' + \left\{ \underline{v}'' \in V'' \,\middle|\, \left\langle \underline{v}'', \sum_{\underline{k}\in\mathcal{O}} f_{\underline{k}}'' \right\rangle = 0 \right\}$$

and

$$C_1'' = \sum_{j=1}^{2p-1} e_j'' + \left\{ \underline{v}'' \in V'' \,\middle|\, \left\langle \underline{v}'', \sum_{\underline{k}\in\mathcal{O}} f_{\underline{k}}'' \right\rangle = 1 \right\}.$$

Finally, the connection sets are given similarly to the previous cases:

$$S'' = \left(\bigcup_i A_i''\right) \cup \left(\bigcup_{\underline{k}\in\mathcal{O}} B_{\underline{k}}''\right) \cup C_0''$$

and

$$T'' = \left(\bigcup_i A_i''\right) \cup \left(\bigcup_{\underline{k}\in\mathcal{O}} B_{\underline{k}}''\right) \cup C_1''$$

and ϕ'' gives the isomorphism between the two Cayley graphs.

Acknowledgements The author is very grateful to Péter P. Pálfy for many valuable suggestions and discussions throughout the preparation of this paper and to the referee for many extremely helpful comments and thorough work.

References

1. Babai, L., Frankl, P.: Isomorphism of Cayley graphs I. In: Colloquia Mathematica Societatis János Bolyai, Keszthely, 1976. Combinatorics, vol. 18, pp. 35–52. North-Holland, Amsterdam (1978)
2. Conder, M., Li, C.H.: On isomorphism of Cayley graphs. Eur. J. Comb. **19**, 911–919 (1998)
3. Hirasaka, M., Muzychuk, M.: An elementary abelian group of rank 4 is a CI-group. J. Comb. Theory, Ser. A **94**(2), 339–362 (2001)
4. Morris, J.: Results towards showing $\mathbb{Z}_p^{2p-1}$ is a CI-group. In: Proceedings of the Thirty-third Southeastern International Conference on Combinatorics, Graph Theory and Computing, Boca Raton, FL, 2002. Congr. Numer, vol. 156, pp. 143–153 (2002)
5. Muzychuk, M.: An elementary abelian group of large rank is not a CI-group. Discrete Math. **264**(1–3), 167–185 (2003)
6. Nowitz, L.A.: A non-Cayley-invariant Cayley graph of the elementary abelian group of order 64. Discrete Math. **110**, 223–228 (1992)
7. Spiga, P.: Elementary abelian p-groups of rank greater than or equal to $4p-2$ are not CI-groups. J. Algebraic Combin. **26**, 343–355 (2007)
8. Spiga, P.: CI-property for elementary abelian 3-groups. Discrete Math. **309**, 3393–3398 (2009)