CONNECTIVITY OF ADDITION CAYLEY GRAPHS

DAVID GRYNKIEWICZ, VSEVOLOD F. LEV, AND ORIOL SERRA

ABSTRACT. For any finite abelian group G and any subset $S \subseteq G$, we determine the connectivity of the addition Cayley graph induced by S on G. Moreover, we show that if this graph is not complete, then it possesses a minimum vertex cut of a special, explicitly described form.

1. BACKGROUND: ADDITION CAYLEY GRAPHS

For a subset S of the abelian group G, we denote by $\mathrm{Cay}_G^+(S)$ the addition Cayley graph induced by S on G; recall that this is the undirected graph with the vertex set G and the edge set $\{(g_1, g_2) \in G \times G \colon g_1 + g_2 \in S\}$. Note that S is not assumed to be symmetric, and that if S is finite, then $\mathrm{Cay}_G^+(S)$ is regular of degree $|S|$ (if one considers each loop to contribute 1 to the degree of the corresponding vertex).

The twins of the usual Cayley graphs, addition Cayley graphs (also called *sum graphs*) received much less attention in the literature; indeed, [A] (independence number), [CGW03] and [L] (hamiltonicity), [C92] (expander properties), and [Gr05] (clique number) is a nearly complete list of papers, known to us, where addition Cayley graphs are addressed. To some extent, this situation may be explained by the fact that addition Cayley graphs are rather difficult to study. For instance, it is well-known and easy to prove that any connected Cayley graph on a finite abelian group with at least three elements is hamiltonian, see [Mr83]; however, apart from the results of [CGW03], nothing seems to be known on hamiltonicity of *addition* Cayley graphs on finite abelian groups. Similarly, the connectivity of a Cayley graph on a finite abelian group is easy to determine, while determining the connectivity of an *addition* Cayley graph is a non-trivial problem, to the solution of which the present paper is devoted. The reader will see that investigating this problem leads to studying rather involved combinatorial properties of the underlying group.

The first author is supported in part by the National Science Foundation, as an MPS-DRF postdoctoral fellow, under grant DMS-0502193.

MSC: 11B75 (05C25, 11P70).

Key Words: addition Cayley graph, sum graph, vertex connectivity, critical pair, sumset.

2. Preliminaries and summary of results

Let Γ be a graph on the finite set V. The (vertex) connectivity of Γ, denoted by $\kappa(\Gamma)$, is the smallest number of vertices which are to be removed from V so that the resulting graph is either disconnected or has only one vertex. Clearly, if Γ is complete, then $\kappa(\Gamma)=|V|-1$, while otherwise we have $\kappa(\Gamma)\le|V|-2$, and $\kappa(\Gamma)$ can be alternatively defined as the size of a minimum vertex cut of Γ. (A complete graph does not have vertex cuts.) Evidently, vertex cuts and connectivity of a graph are not affected by adding or removing loops.

Our goal is to determine the connectivity of the addition Cayley graphs, induced on finite abelian groups by their subsets, and accordingly we use additive notation for the group operation. In particular, for subsets A and B of an abelian group, we write

$$A\pm B:=\{a\pm b\colon a\in A,\, b\in B\},$$

which is abbreviated by $A\pm b$ in the case where $B=\{b\}$ is a singleton subset.

For the rest of this section, we assume that S is a subset of the finite abelian group G.

It is immediate from the definition that, for a subset $A\subseteq G$, the neighborhood of A in $\mathrm{Cay}_G^+(S)$ is the set $S-A$, and it is easy to derive that $\mathrm{Cay}_G^+(S)$ is complete if and only if either $S=G$, or $S=G\setminus\{0\}$ and G is an elementary abelian 2-group (possibly of zero rank). Furthermore, it is not difficult to see that $\mathrm{Cay}_G^+(S)$ is connected if and only if S is not contained in a coset of a proper subgroup of G, with the possible exception of the non-zero coset of a subgroup of index 2; this is [L, Proposition 1]. Also, since $\mathrm{Cay}_G^+(S)$ is $|S|$-regular, we have the trivial bound $\kappa(\mathrm{Cay}_G^+(S))\le|S|$.

If H is a subgroup of G and g is an element of G with $2g\in S+H$, then $g+H\subseteq S-(g+H)$; consequently, the boundary of $g+H$ in $\mathrm{Cay}_G^+(S)$ has size

$$|(S-(g+H))\setminus(g+H)|=|S+H|-|H|.$$

Assuming in addition that $S+H\ne G$, we obtain $(S-(g+H))\cup(g+H)=S+H-g\ne G$, implying $\kappa(\mathrm{Cay}_G^+(S))\le|S+H|-|H|$. Set

$$2*G:=\{2g\colon g\in G\},$$

so that the existence of $g\in G$ with $2g\in S+H$ is equivalent to the condition $(S+2*G)\cap H\ne\varnothing$. Motivated by the above observation, we define

$$\mathcal{H}_G(S):=\{H\le G\colon (S+2*G)\cap H\ne\varnothing,\ S+H\ne G\}$$

and let

$$\eta_G(S):=\min\{|S+H|-|H|\colon H\in\mathcal{H}_G(S)\}.$$

In the latter definition and throughout, we assume that the minimum of an empty set is infinite, and we allow comparison between infinity and real numbers according to the "naıve" rule. Thus, for instance, we have $\kappa(\mathrm{Cay}_G^+(S)) \le \eta_G(S)$ even if $\mathcal{H}_G(S)$ is vacuous.

Another important family of sets with small boundary is obtained as follows. Suppose that the subgroups $L \le G_0 \le G$ and the element $g_0 \in G_0$ satisfy

(i) $|G_0/L|$ is even and larger than 2;
(ii) $S + L = (G \setminus G_0) \cup (g_0 + L)$.

Fix $g \in G_0 \setminus L$ with $2g \in L$ and consider the set $A := (g + L) \cup (g + g_0 + L)$. The neighborhood of this set in $\mathrm{Cay}_G^+(S)$ is

$$S - A = (G \setminus G_0) \cup (g + L) \cup (g + g_0 + L) = (G \setminus G_0) \cup A,$$

whence $(S - A) \cup A \ne G$ and $|(S - A) \setminus A| = |G \setminus G_0| = |S + L| - |L|$. Consequently, $\kappa(\mathrm{Cay}_G^+(S)) \le |S + L| - |L|$. With this construction in mind, we define $\mathcal{L}_G(S)$ to be the family of all those subgroups $L \le G$ for which a subgroup $G_0 \le G$, lying above L, and an element $g_0 \in G_0$ can be found so that properties (i) and (ii) hold, and we let

$$\lambda_G(S) := \min\{|S + L| - |L| \colon L \in \mathcal{L}_G(S)\}.$$

Thus, $\kappa(\mathrm{Cay}_G^+(S)) \le \lambda_G(S)$.

Our first principal result is the following.

Theorem 1. *If S is a proper subset of the finite abelian group G, then*

$$\kappa(\mathrm{Cay}_G^+(S)) = \min\{\eta_G(S), \lambda_G(S), |S|\}.$$

Let Γ be a graph on the vertex set V. We say that the non-empty subset $V_0 \subset V$ is a *fragment* of Γ if the neighborhood $N(V_0)$ of V_0 satisfies $|N(V_0) \setminus V_0| = \kappa(\Gamma)$ and $N(V_0) \cup V_0 \ne V$; that is, the boundary of V_0 is a minimum vertex-cut, separating V_0 from the (non-empty) remainder of the graph. Notice that if Γ is not complete, then it has fragments; for instance, if Γ' is obtained from Γ by removing a minimum vertex cut, then the set of vertices of any connected component of Γ' is a fragment of Γ.

As the discussion above shows, if $\kappa(\mathrm{Cay}_G^+(S)) = \eta_G(S)$, then $\mathrm{Cay}_G^+(S)$ has a fragment which is a coset of a subgroup $H \in \mathcal{H}_G(S)$ with $|S+H|-|H| = \eta_G(S)$; similarly, if $\kappa(\mathrm{Cay}_G^+(S)) = \lambda_G(S)$, then $\mathrm{Cay}_G^+(S)$ has a fragment which is a union of at most two cosets of a subgroup $L \in \mathcal{L}_G(S)$ with $|S + L| - |L| = \lambda_G(S)$.

The reader will easily verify that Theorem 1 is an immediate corollary of Theorem 2 below. The latter shows that the minimum in the statement of Theorem 1 is attained, with just one exception, on either $\eta_G(S)$ or $|S|$. Being much subtler, Theorem 2 is also more technical, and to state it we have to bring into consideration a special subfamily of $\mathcal{L}_G(S)$. Specifically, let $\mathcal{L}^*_G(S)$ be the family of those subgroups $L \le G$ such that for some $G_0 \le G$, lying above L, and some $g_0 \in G_0$, the following conditions hold:

(L1) G_0/L is a cyclic 2-group of order $|G_0/L| \ge 4$, and $\langle g_0 \rangle + L = G_0$;
(L2) G/G_0 is an elementary abelian 2-group (possibly of zero rank);
(L3) $\exp(G/L) = \exp(G_0/L)$;
(L4) $S + L = (G \setminus G_0) \cup (g_0 + L)$ and $S \cap (g_0 + L)$ is not contained in a proper coset of L.

A little meditation shows that $\mathcal{L}^*_G(S) \subseteq \mathcal{L}_G(S)$ and that conditions (L1)–(L3) imply

$$G/L \cong (G_0/L) \oplus (\mathbb{Z}/2\mathbb{Z})^r \cong (\mathbb{Z}/2^k\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^r,$$

for some $k \ge 2$ and $r \ge 0$. Notice also that if L, G_0, and g_0 are as in (L1)–(L4), and $G_0 = G$, then L is a subgroup of G of index at least 4, and S is contained in an L-coset, whence $\mathrm{Cay}^+_G(S)$ is disconnected.

Theorem 2. *Let S be a proper subset of the finite abelian group G. There exists at most one subgroup $L \in \mathcal{L}^*_G(S)$ with $|S + L| - |L| \le |S| - 1$. Moreover,*

(i) *if L is such a subgroup, then $\kappa(\mathrm{Cay}^+_G(S)) = \lambda_G(S) = |S + L| - |L|$ and $\eta_G(S) \ge |S|$;*
(ii) *if such a subgroup does not exist, then $\kappa(\mathrm{Cay}^+_G(S)) = \min\{\eta_G(S), |S|\}$.*

Postponing the proof to Section 4, we now list some of the consequences.

Corollary 1. *Let S be a proper subset of the finite abelian group G such that $\mathrm{Cay}^+_G(S)$ is connected. If either $|S| \le |G|/2$ or G does not contain a subgroup isomorphic to $(\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$, then $\kappa(\mathrm{Cay}^+_G(S)) = \min\{\eta_G(S), |S|\}$.*

Proof. If $\kappa(\mathrm{Cay}^+_G(S)) \ne \min\{\eta_G(S), |S|\}$, then by Theorem 2 there exists $L \in \mathcal{L}^*_G(S)$ with $|S + L| - |L| \le |S| - 1$. Choose $L \le G_0 \le G$ and $g_0 \in G_0$ satisfying (L1)–(L4). Since $\mathrm{Cay}^+_G(S)$ is connected, the subgroup G_0 is proper. Consequently,

$$|S| \ge |S + L| - |L| + 1 = |G| - |G_0| + 1 > \frac{1}{2}\,|G|,$$

and it also follows that G/L contains a subgroup isomorphic to $(\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$, which implies that G itself contains such a subgroup. □

Our next result shows that under the extra assumption $\kappa(\mathrm{Cay}^+_G(S)) < |S|$, the conclusion of Theorem 1 can be greatly simplified.

Theorem 3. *Let S be a proper subset of the finite abelian group G. If $\kappa(\mathrm{Cay}^+_G(S)) < |S|$, then*

$$\kappa(\mathrm{Cay}^+_G(S)) = \min\{|S+H| - |H| \colon H \le G,\ S+H \ne G\}.$$

Theorem 3 will be derived from Theorem 2 in Section 4. Note that the assumption $\kappa(\mathrm{Cay}^+_G(S)) < |S|$ of Theorem 3 cannot be dropped: say, if S is the non-zero coset of a subgroup $H \le G$ of index 2, then $\mathrm{Cay}^+_G(S)$ is a complete bipartite graph of connectivity $|G|/2$, while $|S+H| - |H| = 0$ and $S+H \ne G$. We also notice that, despite its simple and neat conclusion (and one which mirrors the corresponding result for usual Cayley graphs), Theorem 3 gives no way to determine whether $\kappa(\mathrm{Cay}^+_G(S)) < |S|$ holds, and hence no way to find the connectivity unless it is known to be smaller than $|S|$ a priori. Of course, a necessary and sufficient condition for $\kappa(\mathrm{Cay}^+_G(S)) < |S|$ to hold follows readily from Theorem 2.

Corollary 2. *If S is a proper subset of the finite abelian group G, then in order for $\kappa(\mathrm{Cay}^+_G(S)) < |S|$ to hold it is necessary and sufficient that there is a subgroup $K \in \mathcal{H}_G(S) \cup \mathcal{L}^*_G(S)$ with $|S+K| \le |S| + |K| - 1$.*

Observe that if g is an element of G with $2g \in S$, then g is a neighbor of itself in $\mathrm{Cay}^+_G(S)$; consequently, the boundary of $\{g\}$ contains $|S|-1$ elements so that $\kappa(\mathrm{Cay}^+_G(S)) < |S|$. Hence Theorem 3 implies the following corollary.

Corollary 3. *Let S be a proper subset of the finite abelian group G. If $S \cap (2*G) \ne \varnothing$, and in particular if G has odd order and S is non-empty, then*

$$\kappa(\mathrm{Cay}^+_G(S)) = \min\{|S+H| - |H| \colon H \le G,\ S+H \ne G\}.$$

We conclude this section with two potentially useful lower-bound estimates for $\kappa(\mathrm{Cay}^+_G(S))$.

Corollary 4. *Let S be a proper subset of the finite abelian group G. If $\mathrm{Cay}^+_G(S)$ is connected, then in fact*

$$\kappa(\mathrm{Cay}^+_G(S)) \ge \frac{1}{2}\,|S|.$$

Corollary 4 follows from Theorem 3 and the observation that if $|S+H| - |H| = \kappa(\mathrm{Cay}^+_G(S)) > 0$ for a subgroup $H \le G$, then S intersects at least two cosets of H, so that $|S+H| \ge 2|H|$, and therefore $|S+H| - |H| \ge \frac{1}{2}\,|S+H| \ge \frac{1}{2}\,|S|$.

Corollary 5. *Let S be a proper subset of the finite, non-trivial abelian group G, and let p denote the smallest order of a non-zero subgroup of G. If $\mathrm{Cay}^+_G(S)$ is connected, then in fact*

$$\kappa(\mathrm{Cay}^+_G(S)) \ge \min\{|S|-1,\ p\}.$$

The proof is similar to that of the previous corollary: if $\kappa(\mathrm{Cay}_G^+(S)) < |S|-1$, then by Theorem 3 there exists a subgroup $H \le G$ with $|S+H|-|H| = \kappa(\mathrm{Cay}_G^+(S)) > 0$; this subgroup is non-zero and hence $|S+H|-|H| \ge |H| \ge p$.

3. Auxiliary results

In this section, we gather the tools needed for the proof of Theorems 2 and 3. This includes a simple consequence from [Gk01] or [Gk02] (rephrased), a classical theorem of Kneser on periodicity of sumsets, a result from [L05], which is a 'dual' version of a well-known structure theorem of Kemperman [Km60], and three original lemmas.

Given a subgroup H of the abelian group G, by φ_H we denote the canonical homomorphism from G onto G/H. Though the notation φ_H does not specify the underlying group G, it is always implicit from the context and no confusion will arise.

For a subset S of the abelian group G, the (maximal) period of S will be denoted by $\pi(S)$; recall that this is the subgroup of G defined by

$$\pi(S) := \{g \in G \colon S+g = S\},$$

and that S is called *periodic* if $\pi(S) \ne \{0\}$ and *aperiodic* otherwise. Thus, S is a union of $\pi(S)$-cosets, and $\pi(S)$ lies above any subgroup $H \le G$ such that S is a union of H-cosets. Observe also that $\pi(S) = G$ if and only if either $S = \varnothing$ or $S = G$, and that $\varphi_{\pi(G)}(S)$ is an aperiodic subset of the group $G/\pi(S)$.

Proposition A (Grynkiewicz, [Gk01, (c.5)]; see also [Gk02, Proposition 5.2])**.** *Let A be a finite, non-empty subset of an abelian group. If $|\pi(A\setminus\{a\})| > 2$ for some $a \in A$, then $|\pi(A\setminus\{a'\})| = 1$ for every group element $a' \ne a$.*

Theorem A (Kneser, [Kn53, Kn55]; see also [Mn76])**.** *Let A and B be finite, non-empty subsets of an abelian group G. If*

$$|A+B| \le |A|+|B|-1,$$

then, letting $H := \pi(A+B)$, we have

$$|A+B| = |A+H|+|B+H|-|H|.$$

We now turn to the (somewhat involved) statement of [L05, Theorem 2]; the reader can consult the source for the explanations and comments.

By an arithmetic progression in the abelian group G with difference $d \in G$, we mean a set of the form $\{g+d, g+2d, \dots, g+kd\}$, where g is an element of G and k is a positive integer. Thus, cosets of finite cyclic subgroups (and in particular, singleton sets) are considered arithmetic progressions, while the empty set is not. For finite subsets A and B of an abelian group and a group element c, we write

$$\nu_c(A,B) := |\{(a,b) \in A \times B \colon c = a+b\}|;$$

that is, $\nu_c(A,B)$ is the number of representations of c as a sum of an element of A and an element of B. Observe that $\nu_c(A,B) > 0$ if and only if $c \in A+B$. The smallest number of representations of an element of $A+B$ will be denoted by $\mu(A,B)$:

$$\mu(A,B) := \min\{\nu_c(A,B) \colon c \in A+B\}.$$

Following Kemperman [Km60], we say that the pair (A,B) of finite subsets of the abelian group G is *elementary* if at least one of the following conditions holds:

(I) $\min\{|A|,|B|\} = 1$;

(II) A and B are arithmetic progressions sharing a common difference, the order of which in G is at least $|A|+|B|-1$;

(III) $A = g_1 + (H_1 \cup \{0\})$ and $B = g_2 - (H_2 \cup \{0\})$, where $g_1, g_2 \in G$, and where H_1 and H_2 are non-empty subsets of a subgroup $H \le G$ such that $H = H_1 \cup H_2 \cup \{0\}$ is a partition of H; moreover, $c := g_1 + g_2$ is the only element of $A+B$ with $\nu_c(A,B) = 1$;

(IV) $A = g_1 + H_1$ and $B = g_2 - H_2$, where $g_1, g_2 \in G$, and where H_1 and H_2 are non-empty, aperiodic subsets of a subgroup $H \le G$ such that $H = H_1 \cup H_2$ is a partition of H; moreover, $\mu(A,B) \ge 2$.

We say that the pair (A,B) of subsets of an abelian group satisfies *Kemperman's condition* if either $A+B$ is aperiodic or $\mu(A,B) = 1$ holds.

Theorem B (Lev, [L05, Theorem 2])**.** *Let A and B be finite, non-empty subsets of the abelian group G. A necessary and sufficient condition for (A,B) to satisfy both*

$$|A+B| \le |A|+|B|-1$$

and Kemperman's condition is that there exist non-empty subsets $A_0 \subseteq A$ and $B_0 \subseteq B$ and a finite, proper subgroup $F < G$ such that

(i) *each of A_0 and B_0 is contained in an F-coset, $|A_0 + B_0| = |A_0| + |B_0| - 1$, and the pair (A_0, B_0) satisfies Kemperman's condition;*

(ii) *each of $A \setminus A_0$ and $B \setminus B_0$ is a (possibly empty) union of F-cosets;*

(iii) *the pair $(\varphi_F(A), \varphi_F(B))$ is elementary; moreover, either F is trivial, or $\varphi_F(A_0) + \varphi_F(B_0)$ has a unique representation as a sum of an element of $\varphi_F(A)$ and an element of $\varphi_F(B)$.*

Lemma 1. *Let $L \le G_0 \le G$ be finite abelian groups. If G_0/L is a cyclic 2-group and $2 * (G/L)$ is a proper subgroup of G_0/L, then $\exp(G_0/L) = \exp(G/L)$.*

Proof. Write $|G_0/L| = 2^k$ so that k is a positive integer. Since $|2 * (G/L)|$ is a proper divisor of 2^k, we have $2^{k-1}g = 0$ for every $g \in 2 * (G/L)$. Equivalently, $2^k g \in L$ for every $g \in G$, whence $\exp(G/L) \le 2^k = \exp(G_0/L)$. The inverse estimate $\exp(G_0/L) \le \exp(G/L)$ is trivial. □

The following lemma is similar in flavor to a lemma used by Kneser to prove Theorem A; cf. [Kn55, Km60].

Lemma 2. *Suppose that S is a finite subset, and that H and L are finite subgroups of the abelian group G satisfying $|L| \le |H|$ and $S + H \ne S + H + L$. Let $I := H \cap L$. If*

$$\max\{|S + H| - |H|, |S + L| - |L|\} \le |S + I| - |I|,$$

then in fact

$$|S + H| - |H| = |S + L| - |L| = |S + I| - |I|;$$

moreover, there exists $g \in G$ such that $(S + I) \setminus (g + H + L)$ is a (possibly empty) union of $(H + L)$-cosets, and one of the following holds:

(i) $(S + I) \cap (g + H + L) = g + I$*;*
(ii) $(S + I) \cap (g + H + L) = (g + H + L) \setminus (g + (H \cup L))$ *and* $|H| = |L|$*.*

Proof. Factoring by I, we assume without loss of generality that $I = \{0\}$. Since $S + H \ne S + H + L$, there exists $s_0 \in S$ with $s_0 + L \nsubseteq S + H$, and we let $S_0 := S \cap (s_0 + H + L)$. It is instructive to visualize the coset $s_0 + H + L$ as the grid formed by $|L|$ horizontal lines (corresponding to the H-cosets contained in $s_0 + H + L$) and $|H|$ vertical lines (corresponding to the L-cosets contained in $s_0 + H + L$). The intersection points of these two families of lines correspond to the elements of $s_0 + H + L$, and the condition $s_0 + L \nsubseteq S + H$ implies that there is a horizontal line free of elements of S.

Let $h := \varphi_L(S_0)$ (the number of vertical lines that intersect S_0) and $l := \varphi_H(S_0)$ (the number of horizontal lines that intersect S_0); thus, $1 \le h \le |H|$ and $1 \le l < |L|$. We also have, in view of the hypotheses,

$$(|H| - h)l \le |(S_0 + H) \setminus S_0| \le |(S + H) \setminus S| \le |H| - 1, \tag{1}$$

whence

$$(|H| - h)(l - 1) \le h - 1, \tag{2}$$

and similarly,

$$(|L| - l)(h - 1) \le l - 1. \tag{3}$$

To begin with, suppose that $l = 1$, and hence $h = 1$ by (3). In this case, $|S_0| = 1$, whence $S \cap (s_0 + H + L) = \{s_0\}$. Furthermore, (1) yields $(S_0 + H) \setminus S_0 = (S + H) \setminus S$, and likewise we have $(S_0 + L) \setminus S_0 = (S + L) \setminus S$. This shows that

$$|S + H| - |S| = |H| - 1, \quad |S + L| - |S| = |L| - 1, \tag{4}$$

and $S \setminus S_0$ is a union of $(H + L)$-cosets, thus establishing the assertion (with $g = s_0$) in the case $l = 1$. So we assume $l > 1$ below.

Observe that (2) and (3) imply

$$l - 1 \geq (|L| - l)(h - 1) \geq (|L| - l)(|H| - h)(l - 1),$$

whence it follows from $l > 1$ that

$$(|L| - l)(|H| - h) \leq 1. \tag{5}$$

If $|H| = h$, then (3) gives

$$l - 1 \geq (|H| - 1)(|L| - l) \geq (|L| - 1)(|L| - l) \geq 2|L| - l - 2 \geq l,$$

which is wrong. Therefore $|H| > h$. Thus we deduce from (5) and $l < |L|$ that $h = |H| - 1$ and $l = |L| - 1$, whence (3) gives $|H| = |L|$. Consequently, (1) yields $(S_0 + H) \setminus S_0 = (S + H) \setminus S$, and similarly $(S_0 + L) \setminus S_0 = (S + L) \setminus S$, which (as above) proves (4) and shows that $S \setminus S_0$ is a union of $(H + L)$-cosets. Furthermore, $S + H$ misses exactly one H-coset in $s_0 + H + L$, and $S + L$ misses exactly one L-coset in $s_0 + H + L$. Let $g \in s_0 + H + L$ be the common element of these two cosets, so that $S_0 + H = (s_0 + H + L) \setminus (g + H)$ and $S_0 + L = (s_0 + H + L) \setminus (g + L)$. Then

$$S_0 \subseteq (s_0 + H + L) \setminus (g + (H \cup L)) = (g + H + L) \setminus (g + (H \cup L)),$$

and thus

$$|L| - 1 = |H| - 1 \geq |(S + H) \setminus S| = |(S_0 + H) \setminus S_0| = (|L| - 1)|H| - |S_0|,$$

so that

$$|S_0| \geq (|H| - 1)(|L| - 1) = |(g + H + L) \setminus (g + (H \cup L))|.$$

Hence, in fact $S_0 = (g + H + L) \setminus (g + (H \cup L))$, completing the proof. □

Lemma 3. *Let G be a finite abelian group, and suppose that the proper subset $S \subset G$, the subgroups $L \leq G_0 \leq G$, and the element $g_0 \in G_0$ satisfy conditions (L1)–(L4) in the definition of $\mathcal{L}^*_G(S)$. Suppose, moreover, that $|S + L| - |S| \leq |L| - 1$. If H is a subgroup of G with $|S + H| - |S| \leq |H| - 1$ and $S + H \neq G$, then H is actually a subgroup of G_0.*

Proof. Suppose for a contradiction that $H \nleq G_0$ and fix $h \in H \setminus G_0$. For each $g \in G_0$, we have $g + h \in G \setminus G_0 \subseteq S + L$, whence $g \in S + H + L$. Hence $G_0 \subseteq S + H + L$, and since, on the other hand, we have $G \setminus G_0 \subseteq S + L \subseteq S + H + L$, we conclude that

$$S + H + L = G. \tag{6}$$

In view of $S+H\neq G$, this leads to $L\nleq H$, and we let $I:=H\cap L$. Thus I is a proper subgroup of L.

Write $n:=|G_0/L|$ so that G_0 consists of $n\geq 4$ cosets of L, of which $n-1$ are free of elements of S. Let $\{g_i\colon 0\leq i\leq n-1\}$ be a system of representatives of these n cosets.

Fix $i\in[1,n-1]$. Since $H\nleq G_0$ and $g_i\in G_0$, we have $g_i+H\nsubseteq G_0$, whence $(G\setminus G_0)\cap(g_i+H)\neq\varnothing$; as $G\setminus G_0\subseteq S+L$, this yields $S\cap(g_i+H+L)\neq\varnothing$. On the other hand, from $g_i+L\subseteq G_0\setminus(g_0+L)$ it follows that $(S+L)\cap(g_i+L)=\varnothing$. Therefore,

$$0<|(S+I)\cap(g_i+H+L)|<|H+L|;\quad i\in[1,n-1]. \tag{7}$$

In view of (6) and the hypotheses $S+H\neq G$, we have $S+H\neq S+H+L$ and $S+L\neq S+H+L$. Also, our assumptions imply

$$\max\{|S+H|-|H|,|S+L|-|L|\}<|S|\leq|S+I|,$$

and since both the left and right hand side are divisible by $|I|$, we actually have

$$\max\{|S+H|-|H|,|S+L|-|L|\}\leq|S+I|-|I|.$$

Thus we can apply Lemma 2. Choose $g\in G$ such that $(S+I)\setminus(g+H+L)$ is a union of $(H+L)$-cosets. Then it follows from (7) that

$$g_i+H+L=g+H+L;\quad i\in[1,n-1], \tag{8}$$

and consequently $G_0\setminus(g_0+L)\subseteq g+H+L$. Hence $n\geq 4$ implies $G_0\leq H+L$ and $g\in H+L$. Thus, since $S\cap(g_0+L)$ is not contained in a coset of a proper subgroup of L, and in particular in a coset of I, we conclude that

$$|(S+I)\cap(g+H+L)|=|(S+I)\cap(g_0+L)|\geq 2|I|.$$

This shows that Lemma 2 (i) fails. On the other hand, (8) gives $g_i+L\subseteq g+H+L$, and hence $g+H+L$ contains at least $n-1\geq 3$ cosets of L, all free of elements of $S+I$. Thus Lemma 2 (ii) fails too, a contradiction. □

4. Proofs of Theorems 2 and 3

Our starting point is the observation that if S is a subset of the finite abelian group G such that $\mathrm{Cay}^+_G(S)$ is not complete, then

$$\kappa(\mathrm{Cay}^+_G(S))=\min\{|(S-A)\setminus A|\colon\varnothing\neq A\subseteq G,\,(S-A)\cup A\neq G\}.$$

For the following proposition, the reader may need to recall the notion of a fragment, introduced in Section 2 after the statement of Theorem 1.

Proposition 1. *Let S be a subset of the finite abelian group G, and suppose that $\kappa(\mathrm{Cay}^+_G(S)) < |S|$. If A is a fragment of $\mathrm{Cay}^+_G(S)$, then, writing $H := \pi(S-A)$, we have*

$$A \subseteq S - A, \tag{9}$$

$$A + H = A, \tag{10}$$

$$\kappa(\mathrm{Cay}^+_G(S)) = |S+H| - |H|, \tag{11}$$

and

$$\kappa(\mathrm{Cay}^+_{G/H}\,\varphi_H(S)) = |\varphi_H(S)| - 1. \tag{12}$$

Proof. Fix $a \in A$. Since a has $|S|$ neighbors, all lying in $S-A$, and since $|(S-A)\setminus A| = \kappa(\mathrm{Cay}^+_G(S)) < |S|$ by the assumptions, it follows that a has a neighbor in A; in other words, there is $a' \in A$ with $a + a' \in S$. Consequently, $a \in S - A$, and (9) follows.

By (9) we have

$$(S - (A+H)) \cup (A+H) = S - A + H = S - A \neq G,$$

and obviously,

$$|(S-(A+H)) \setminus (A+H)| = |(S-A) \setminus (A+H)| \leq |(S-A) \setminus A|.$$

Since A is a fragment, we conclude that in fact $|(S-A)\setminus(A+H)| = |(S-A)\setminus A|$ holds, which gives (10).

By (9) and the assumptions, we have

$$|S-A| = |(S-A)\setminus A| + |A| = \kappa(\mathrm{Cay}^+_G(S)) + |A| \leq |S| + |A| - 1.$$

Hence it follows from Theorem A and (10) that

$$|S-A| = |S+H| + |A+H| - |H| = |S+H| + |A| - |H|. \tag{13}$$

Thus

$$\kappa(\mathrm{Cay}^+_G(S)) = |(S-A)\setminus A| = |S-A| - |A| = |S+H| - |H|,$$

yielding (11).

Finally, we establish (12). The neighborhood of $\varphi_H(A)$ in the graph $\mathrm{Cay}^+_{G/H}(\varphi_H(S))$ is $\varphi_H(S) - \varphi_H(A) = \varphi_H(S-A)$, and it follows in view of (9) that

$$\varphi_H(S-A) \cup \varphi_H(A) = \varphi_H(S-A) \neq G/H.$$

Consequently, the set $\varphi_H(S-A)\setminus\varphi_H(A)$ is a vertex cut in $\mathrm{Cay}^+_{G/H}(\varphi_H(S))$, whence using (9), (10), and (13) we obtain

$$\begin{aligned}\kappa(\mathrm{Cay}^+_{G/H}(\varphi_H(S))) &\leq |\varphi_H(S-A)\setminus\varphi_H(A)| = |\varphi_H(S-A)| - |\varphi_H(A)| \\ &= (|S-A| - |A|)/|H| = |S+H|/|H| - 1 = |\varphi_H(S)| - 1.\end{aligned}$$

To prove the inverse estimate, notice that the graph $\mathrm{Cay}^+_{G/H}(\varphi_H(S))$ is not complete (we saw above that it has vertex cuts) and choose $A' \subseteq G$ such that $\varphi_H(A')$ is a fragment of this graph. Replacing A' with $A'+H$, we can assume without loss of generality that $A'+H=A'$. Since

$$\varphi_H((S-A')\cup A') = (\varphi_H(S)-\varphi_H(A'))\cup\varphi_H(A') \neq G/H,$$

we have $(S-A')\cup A' \neq G$. Hence in view of (11) it follows that

$$\begin{aligned}\kappa(\mathrm{Cay}^+_{G/H}(\varphi_H(S))) &= |(\varphi_H(S)-\varphi_H(A'))\setminus\varphi_H(A')| \\ &= |\varphi_H(S-A')\setminus\varphi_H(A')| \\ &= |(S-A')\setminus A'|/|H| \\ &\geq |\kappa(\mathrm{Cay}^+_G(S))|/|H| \\ &= |\varphi_H(S)|-1,\end{aligned}$$

as desired. □

For a subset S of a finite abelian group G, write

$$\lambda^*_G(S) := \min\{|S+L|-|L| \colon L\in\mathcal{L}^*_G(S)\}.$$

Clearly, we have $\lambda^*_G(S)\geq\lambda_G(S)$.

Lemma 4. *Let S be a proper subset of the finite abelian group G. If $g\in G$, then $\mathcal{H}_G(S-2g)=\mathcal{H}_G(S)$, $\mathcal{L}^*_G(S-2g)=\mathcal{L}^*_G(S)$, and $\mathrm{Cay}^+_G(S-2g)$ is isomorphic to $\mathrm{Cay}^+_G(S)$; consequently,*

$$\eta_G(S-2g)=\eta_G(S),\ \ \lambda^*_G(S-2g)=\lambda^*_G(S),$$

and

$$\kappa(\mathrm{Cay}^+_G(S-2g))=\kappa(\mathrm{Cay}^+_G(S)).$$

Proof. The isomorphism between $\mathrm{Cay}^+_G(S-2g)$ and $\mathrm{Cay}^+_G(S)$ is established by mapping every group element x to $x-g$, and the equality $\mathcal{H}_G(S-2g)=\mathcal{H}_G(S)$ is immediate from the observation that $S+2*G-2g=S+2*G$. To show that $\mathcal{L}^*_G(S-2g)=\mathcal{L}^*_G(S)$, suppose that $L\in\mathcal{L}^*_G(S)$ and let $G_0\leq G$ (lying above L) and $g_0\in G_0$ be as in (L1)–(L4). By (L2) we have $2g\in G_0$. Consequently, $(G\setminus G_0)-2g=G\setminus G_0$, and hence it follows from (L4) that

$$S-2g+L=(G\setminus G_0)\cup(g_0-2g+L).$$

Furthermore, since $\varphi_L(g_0)$ is a generator of the cyclic 2-group G_0/L, so is $\varphi_L(g_0-2g)$; that is, $\langle g_0-2g\rangle+L=G_0$. This shows that $L\in\mathcal{L}^*_G(S-2g)$, and hence

$\mathcal{L}^*_G(S) \subseteq \mathcal{L}^*_G(S-2g)$. By symmetry, we also have $\mathcal{L}^*_G(S-2g) \subseteq \mathcal{L}^*_G(S)$, implying the assertion. $\square$

We now pass to our last lemma, which will take us most of the way towards the proof of Theorem 2; the reader may compare the statement of this lemma with that of Theorem 1.

Lemma 5. *If S is a proper subset of the finite abelian group G, then*

$$\kappa(\mathrm{Cay}^+_G(S)) = \min\{\eta_G(S), \lambda^*_G(S), |S|\}. \tag{14}$$

Proof. Since each of $\eta_G(S)$, $\lambda^*_G(S)$, and $|S|$ is an upper bound for $\kappa(\mathrm{Cay}^+_G(S))$, it suffices to show that $\kappa(\mathrm{Cay}^+_G(S))$ is greater than or equal to one of these quantities. Thus we can assume that $\kappa(\mathrm{Cay}^+_G(S)) \le |S|-1 \le |G|-2$. Hence $S \ne \varnothing$ and $\mathrm{Cay}^+_G(S)$ is not complete.

It is not difficult to see that the assertion holds true if $|G| \le 2$; we leave verification to the reader. The case $|S| = 1$ is also easy to establish as follows. Suppose that $|G| > 2$ and $S = \{s\}$, where s is an element of G. If $\langle s\rangle \ne G$, then $\langle s\rangle \in \mathcal{H}_G(S)$ and $|S + \langle s\rangle| - |\langle s\rangle| = 0$, implying $\kappa(\mathrm{Cay}^+_G(S)) = \eta_G(S) = 0$. Next, if G is not a 2-group, then there exists an element $g \in G$ which is an odd multiple of s and such that the subgroup $\langle g\rangle$ is proper; in this case $g \in (S + 2 * G) \cap \langle g\rangle$ showing that $\langle g\rangle \in \mathcal{H}_G(S)$ and leading to $\kappa(\mathrm{Cay}^+_G(S)) = \eta_G(S) = 0$, as above. In both cases the proof is complete, so we assume that $\langle s\rangle = G$ is a 2-group. Since $|G| > 2$, in this case we have $\{0\} \in \mathcal{L}^*_G(S)$ (take $G_0 = G$ and $g_0 = s$ in (L1)–(L4)) and $|S+\{0\}|-|\{0\}| = 0$, whence $\kappa(\mathrm{Cay}^+_G(S)) = \lambda^*_G(S) = 0$.

Having finished with the cases $|S| = 1$ and $|G| \le 2$, we proceed by induction on $|G|$, assuming that $\kappa(\mathrm{Cay}^+_G(S)) \le |S| - 1$. Choose $A \subseteq G$ such that A is a fragment of $\mathrm{Cay}^+_G(S)$ and fix arbitrarily $a \in A$. In view of Lemma 4, and since the set $A - a$ is a fragment of the graph $\mathrm{Cay}^+_G(S - 2a)$, by passing from S to $S - 2a$, and from A to $A - a$, we ensure that

$$0 \in A. \tag{15}$$

Also, by Proposition 1 we have $A \subseteq S - A \ne G$.

If each of S and A is contained in a coset of a proper subgroup $K < G$, then from $A \subseteq S - A$ and (15) it follows that in fact S and A are contained in K, whence $K \in \mathcal{H}_G(S)$; furthermore, $|S + K| - |K| = 0$, showing that $\kappa(\mathrm{Cay}^+_G(S)) = \eta_G(S) = 0$. Accordingly, we assume for the rest of the proof that for any proper subgroup of G, at least one of the sets S and A is not contained in a coset of this subgroup.

Let $H := \pi(S - A)$. We distinguish two major cases according to whether or not H is trivial.

Case 1: H is non-trivial. Applying the induction hypothesis to $\mathrm{Cay}^+_{G/H}(\varphi_H(S))$ and using (12), we conclude that either $\eta_{G/H}(\varphi_H(S)) = |\varphi_H(S)| - 1$ or $\lambda^*_{G/H}(\varphi_H(S)) = |\varphi_H(S)| - 1$, giving two subcases.

Subcase 1.1. Assume first that $\eta_{G/H}(\varphi_H(S)) = |\varphi_H(S)| - 1$, and hence that there exists a subgroup $H' \le G$, lying above H, such that $H'/H \in \mathcal{H}_{G/H}(\varphi_H(S))$ and

$$|\varphi_H(S) + H'/H| - |H'/H| = \eta_{G/H}(\varphi_H(S)) = |\varphi_H(S)| - 1.$$

The former easily implies that $H' \in \mathcal{H}_G(S)$, while the latter, in conjunction with (11), implies that

$$|S + H'| - |H'| = |S + H| - |H| = \kappa(\mathrm{Cay}^+_G(S)).$$

This shows that $\kappa(\mathrm{Cay}^+_G(S)) \ge \eta_G(S)$, whence in fact $\kappa(\mathrm{Cay}^+_G(S)) = \eta_G(S)$.

Subcase 1.2. Assume now that $\lambda^*_{G/H}(\varphi_H(S)) = |\varphi_H(S)| - 1$, and let $L \le G$ be a subgroup, lying above H, such that $L/H \in \mathcal{L}^*_{G/H}(\varphi_H(S))$ and

$$|\varphi_H(S) + L/H| - |L/H| = \lambda^*_{G/H}(\varphi_H(S)) = |\varphi_H(S)| - 1.$$

In view of (11) and the assumptions, the last equality yields

$$|S + L| - |L| = |S + H| - |H| = \kappa(\mathrm{Cay}^+_G(S)) \le |S| - 1. \tag{16}$$

Since $L/H \in \mathcal{L}^*_{G/H}(\varphi_H(S))$, we can find a subgroup $G_0 \le G$, lying above L, and an element $g_0 \in G_0 \setminus L$, so that G/G_0 is an elementary abelian 2-group, G_0/L is a cyclic 2-group of order at least 4 generated by $\varphi_L(g_0)$, and $S + L = (G \setminus G_0) \cup (g_0 + L)$. Without loss of generality, we can assume that $g_0 \in S$.

If $S_0 := S \cap (g_0 + L)$ is not contained in a coset of a proper subgroup of L, then $L \in \mathcal{L}^*_G(S)$, and hence it follows in view of (16) that $\kappa(\mathrm{Cay}^+_G(S)) = \lambda^*_G(S)$. Therefore we assume that there exists a proper subgroup $R < L$ such that S_0 is contained in an R-coset, and we choose R to be minimal subject to this property; thus, $S_0 = S \cap (g_0 + R)$ and $\langle (S - g_0) \cap L \rangle = R$.

Since S_0 is contained in an R-coset, from (16) we obtain

$$|(S \setminus S_0) + L| - |S \setminus S_0| = |S + L| - |L| - |S| + |S_0| < |S_0| \le |R|.$$

Hence every R-coset in $G \setminus G_0 = (S \setminus S_0) + L$ contains at least one element of S; that is,

$$S + R = (G \setminus G_0) \cup (g_0 + R). \tag{17}$$

Consequently, using (16) once again, we obtain

$$|S + R| - |R| = |G \setminus G_0| = |S + L| - |L| = \kappa(\mathrm{Cay}^+_G(S)). \tag{18}$$

Applying the previously completed singleton case to the set $\varphi_R(S_0) \subseteq G_0/R$, we get two further subcases.

Subcase 1.2.1. Suppose that $\kappa(\mathrm{Cay}^+_{G_0/R}(\varphi_R(S_0))) = \eta_{G_0/R}(\varphi_R(S_0))$. Choose a subgroup $R' \le G_0$, lying above R, such that $R'/R \in \mathcal{H}_{G_0/R}(\varphi_R(S_0))$. Since $R \le R' \le G_0$, it follows in view of (17) and (18) that

$$|S + R'| - |R'| = |S + R| - |R| = \kappa(\mathrm{Cay}^+_G(S)).$$

Thus, since $R' \in \mathcal{H}_{G_0}(S_0) \subseteq \mathcal{H}_G(S)$, we conclude that $\kappa(\mathrm{Cay}^+_G(S)) = \eta_G(S)$.

Subcase 1.2.2. Assume now that $\kappa(\mathrm{Cay}^+_{G_0/R}(\varphi_R(S_0))) \ne \eta_{G_0/R}(\varphi_R(S_0))$. As $|G_0/R| \ge |G_0/L| \ge 4$, from the singleton case analysis at the beginning of the proof it follows that G_0/R is a cyclic 2-group generated by $\varphi_R(S_0) = \{\varphi_R(g_0)\}$.

If $R \in \mathcal{H}_G(S)$, then it follows in view of (18) that $\kappa(\mathrm{Cay}^+_G(S)) = \eta_G(S)$; therefore, we assume that $R \notin \mathcal{H}_G(S)$. Hence in view of $S + R \subseteq S + L \ne G$ we infer that $2 * (G/R) \cap \varphi_R(S) = \varnothing$. Consequently, since (17) implies that $\varphi_R(S)$ contains $(G/R) \setminus (G_0/R)$ as a proper subset, we have $2 * (G/R) \subsetneqq G_0/R$.

Applying Lemma 1, we conclude that $\exp(G_0/R) = \exp(G/R)$. Thus (17), the remark at the beginning of the present subcase, and the above-made observation that G/G_0 is an elementary 2-group show that $R \in \mathcal{L}^*_G(S)$, whence (18) yields $\kappa(\mathrm{Cay}^+_G(S)) = \lambda^*_G(S)$.

Case 2: H is trivial. Thus by (11) we have $\kappa(\mathrm{Cay}^+_G(S)) = |S| - 1$, and therefore (9) gives

$$|S - A| - |A| = |(S - A) \setminus A| = \kappa(\mathrm{Cay}^+_G(S)) = |S| - 1.$$

Applying Theorem B to the pair $(S, -A)$, we find a subgroup $F < G$ such that conclusions (i)–(iii) of Theorem B hold true; in particular, $(\varphi_F(S), -\varphi_F(A))$ is an elementary pair in G/F of one of the types (I)–(IV), and $|S + F| \le |S| + |F| - 1$. By the last inequality, we have

$$|S + F| - |F| \le |S| - 1 = \kappa(\mathrm{Cay}^+_G(S)).$$

Hence, if $F \in \mathcal{H}_G(S)$, then $\kappa(\mathrm{Cay}^+_G(S)) = \eta_G(S)$; consequently, we assume that

$$F \notin \mathcal{H}_G(S). \tag{19}$$

Observe that if $\varphi_F(S) = G/F$, then F is non-zero, whence by Theorem B (iii) we have $|\varphi_F(A)| = 1$. Thus, if $(\varphi_F(S), -\varphi_F(A))$ is not of type (I), then

$$S + F \ne G. \tag{20}$$

We proceed by cases corresponding to the type of the pair $(\varphi_F(S), -\varphi_F(A))$.

Subcase 2.1. Suppose that $(\varphi_F(S), -\varphi_F(A))$ is of type (IV). In this case, we have $\mu(\varphi_F(S), -\varphi_F(A)) \geq 2$, whence it follows by Theorem B (iii) that F is trivial. Hence $(S, -A)$ is an elementary pair of type (IV). Thus, since S and A are not both contained in a coset of the same proper subgroup, it follows that $A = g + (G \setminus S)$ for some $g \in G$, implying $-g \notin S - A$. Therefore (9) yields $-g \notin g + (G \setminus S)$ and thus $-2g \in S$; consequently, $\{0\} = F \in \mathcal{H}_G(S)$, contradicting (19).

Subcase 2.2. Suppose that $(\varphi_F(S), -\varphi_F(A))$ is of type (III), but not of type (I). Then, since S and A are not both contained in a coset of the same proper subgroup and since $S - A \neq G$, it follows that F is non-zero, that

$$\varphi_F(S) = \varphi_F(g_1) + (H_1 \cup \{0\}),\ -\varphi_F(A) = \varphi_F(g_2) - (H_2 \cup \{0\})$$

for some $g_1, g_2 \in G$, where $H_1 \cup H_2 \cup \{0\}$ is a partition of G/F, and that $g_1 + g_2 + F$ has a non-empty intersection with $S - A$, while every F-coset, other than $g_1 + g_2 + F$, is contained in $S - A$; moreover, from $\pi(S - A) = \{0\}$ we derive that

$$g_1 + g_2 + F \nsubseteq S - A. \tag{21}$$

By Theorem B, all F-cosets corresponding to

$$(-\varphi_F(A)) \setminus \{\varphi_F(g_2)\} = \varphi_F(g_2) - H_2,$$

are contained in $-A$. Hence, if

$$-\varphi_F(g_1 + g_2) \in \varphi_F(g_2) - H_2,$$

then $-g_1 - g_2 + F \subseteq -A$, and it follows in view of (9) that $g_1 + g_2 + F \subseteq A \subseteq S - A$, contradicting (21). Therefore, assume instead that $-\varphi_F(g_1 + g_2) \notin \varphi_F(g_2) - H_2$, so that $\varphi_F(g_1 + 2g_2) \in H_1 \cup \{0\}$. Then $2\varphi_F(g_1 + g_2) \in \varphi_F(g_1) + (H_1 \cup \{0\}) = \varphi_F(S)$, whence by (20) we have $F \in \mathcal{H}_G(S)$, contradicting (19).

Subcase 2.3. Suppose that $(\varphi_F(S), -\varphi_F(A))$ is of type (II), but not of type (I). Letting $u := |\varphi_F(S)|$ and $v := |\varphi_F(A)|$, and choosing $s_0 \in S$, $a_0 \in A$, and $d \in G \setminus \{0\}$ appropriately, we write

$$\varphi_F(S) = \{\varphi_F(s_0), \varphi_F(s_0) + \varphi_F(d), \dots, \varphi_F(s_0) + (u-1)\varphi_F(d)\}$$

and

$$-\varphi_F(A) = \{\varphi_F(a_0), \varphi_F(a_0) + \varphi_F(d), \dots, \varphi_F(a_0) + (v-1)\varphi_F(d)\}.$$

Since $(\varphi_F(S), -\varphi_F(A))$ is not of type (I), we have $u,\, v \geq 2$. Next, it follows from (9) that

$$-\varphi_F(a_0) = \varphi_F(s_0) + \varphi_F(a_0) + r\varphi_F(d),$$

and therefore $\varphi_F(s_0) = -2\varphi_F(a_0) - r\varphi_F(d)$, for some integer r. Thus either $\varphi_F(s_0)$ (if r is even) or $\varphi_F(s_0) + \varphi_F(d)$ (if r is odd) belongs to $2 * (G/F)$. In either case, in view of $u \geq 2$ we have $\varphi_F(S) \cap (2 * (G/F)) \neq \varnothing$, which by (20) leads to $F \in \mathcal{H}_G(S)$, contradicting (19).

Subcase 2.4. Finally, suppose that $(\varphi_F(S), -\varphi_F(A))$ is of type (I); that is, either $|\varphi_F(S)| = 1$ or $|\varphi_F(A)| = 1$ holds.

Suppose first that $|\varphi_F(S)| = 1$. In this case, F is non-zero (as $|S| > 1$) and $S + F \neq G$ (as F is a *proper* subgroup); moreover, from (9) we obtain

$$\varphi_F(S) - \varphi_F(A) = \varphi_F(A). \tag{22}$$

By Theorem B, we can write $A = A_1 \cup A_0$, where A_1 is a union of F-cosets and A_0 is a non-empty subset of an F-coset disjoint from A_1. If $\varphi_F(S) - \varphi_F(A_0) \subseteq \varphi_F(A_1)$, then $S - A_0 + F \subseteq A_1 + F = A_1 \subseteq S - A$, whence $S - A = (S - A_1) \cup (S - A_0)$ is a union of F-cosets, contradicting the assumption that $S - A$ is aperiodic. Therefore (22) gives $\varphi_F(S) - \varphi_F(A_0) = \varphi_F(A_0)$, which together with $S + F \neq G$ implies $F \in \mathcal{H}_G(S)$, contradicting (19). So we assume for the remainder of the proof that $|\varphi_F(S)| > |\varphi_F(A)| = 1$, and consequently in view of (15) that $A \subseteq F$.

Thus from (9) we derive that $0 \in \varphi_F(S)$, and it follows in view of (19) that $S + F = G$. Hence F is nontrivial, and Theorem B shows that there exists $s_0 \in S$ such that $S = (G \setminus (s_0 + F)) \cup S_0$, where $S_0 \subset s_0 + F$.

If there exists $g \in G$ with $\varphi_F(g) \neq -\varphi_F(g) + \varphi_F(s_0)$, then it follows in view of $\varphi_F(S) = G/F$ that $\varphi_F(g) \in -\varphi_F(g) + \varphi_F(S \setminus S_0)$, whence

$$g \in -g + (S \setminus S_0) + F \subseteq -g + S;$$

consequently, $\{0\} \in \mathcal{H}_G(S)$ and $\kappa(\mathrm{Cay}^+_G(S)) = \eta_G(S)$. Therefore we assume that $\varphi_F(g) = -\varphi_F(g) + \varphi_F(s_0)$ for all $g \in G$. Hence $2 * (G/F) = \{\varphi_F(s_0)\}$, which implies that G/F is an elementary 2-group and that $\varphi_F(s_0) = 0$; consequently, $S_0 = S \cap F$.

From $A \subseteq F$ and (9), it follows that $A \subseteq (S-A) \cap F = S_0 - A$, and since $S - A \neq G$ and $S + F = G$ we have $S_0 - A \neq F$. Consequently, Theorem B (i) yields

$$\kappa(\mathrm{Cay}^+_F(S_0)) \leq |(S_0 - A) \setminus A| = |S_0 - A| - |A| \leq |S_0| - 1. \tag{23}$$

Since S_0 is a proper subset of F, it follows in view of (23) that $\kappa(\mathrm{Cay}^+_F(S_0)) \leq |F| - 2$, whence $\mathrm{Cay}^+_F(S_0)$ is not complete. Let $A' \subseteq F$ be a fragment of $\mathrm{Cay}^+_F(S_0)$. By (9) and 23, we have $A' \subseteq S_0 - A' \neq F$, and consequently $A' \subseteq S - A' \neq G$. Hence from (23) and $S \setminus S_0 = G \setminus F$ we obtain

$$\begin{aligned} |S| - 1 = \kappa(\mathrm{Cay}^+_G(S)) \leq |(S - A') \setminus A'| &\leq |G \setminus F| + |(S_0 - A') \setminus A'| \\ &= |S \setminus S_0| + \kappa(\mathrm{Cay}^+_F(S_0)) \leq |S| - 1, \end{aligned}$$

implying $\kappa(\mathrm{Cay}_F^+(S_0)) = |S_0| - 1$ and

$$\kappa(\mathrm{Cay}_G^+(S)) = |S \setminus S_0| + \kappa(\mathrm{Cay}_F^+(S_0)).$$

Consequently, if $F' \le F$ has the property that $\kappa(\mathrm{Cay}_F^+(S_0)) = |S_0 + F'| - |F'|$, then

$$\kappa(\mathrm{Cay}_G^+(S)) = |S + F'| - |F'|. \tag{24}$$

With (23) in mind, we apply the induction hypothesis to the graph $\mathrm{Cay}_F^+(S_0)$. If $\kappa(\mathrm{Cay}_F^+(S_0)) = \eta_F(S_0)$, then by (24) any subgroup $F' \in \mathcal{H}_F(S_0) \subseteq \mathcal{H}_G(S)$ with $\kappa(\mathrm{Cay}_F^+(S_0)) = |S_0 + F'| - |F'|$ satisfies $\kappa(\mathrm{Cay}_G^+(S)) = |S + F'| - |F'|$, whence $\kappa(\mathrm{Cay}_G^+(S)) = \eta_G(S)$. Therefore we assume instead that $\kappa(\mathrm{Cay}_F^+(S_0)) = \lambda_F^*(S_0)$.

Choose $L \in \mathcal{L}_F^*(S_0)$ with $\lambda_F^*(S_0) = |S_0 + L| - |L|$, and let G_0 and $g_0 \in G_0$ be as in (L1)–(L4), with F playing the role of G. Then it follows in view of (24) that

$$\kappa(\mathrm{Cay}_G^+(S)) = |S + L| - |L|. \tag{25}$$

If $\varphi_L(S) \cap 2 * (G/L) \neq \varnothing$, then $L \in \mathcal{H}_G(S)$, whence (25) yields $\kappa(\mathrm{Cay}_G^+(S)) = \eta_G(S)$. Therefore we assume that

$$\varphi_L(S) \cap 2 * (G/L) = \varnothing \tag{26}$$

and we proceed to show that $L \in \mathcal{L}_G^*(S)$; in view of (25), this will complete the proof.

Since $L \in \mathcal{L}_F^*(S_0)$, and by the choice of G_0 and g_0, we see that G_0/L is a cyclic 2-group with $|G_0/L| \ge 4$ and $\langle g_0 \rangle + L = G_0$; furthermore, $S \cap (g_0 + L)$ is not contained in a proper coset of L, and $S_0 + L = (F \setminus G_0) \cup (g_0 + L)$, which in view of $S = (G \setminus F) \cup S_0$ and $L \le F$ yields

$$S + L = (G \setminus G_0) \cup (g_0 + L). \tag{27}$$

It remains to show that $\exp(G/L) = \exp(G_0/L)$ and that G/G_0 is an elementary 2-group. To prove the former, we observe that (26) and (27) yield $2 * (G/L) \subsetneqq G_0/L$ and invoke Lemma 1. To establish the latter, simply observe that $2 * (G/L) \subsetneqq G_0/L$ implies $2 * G \le G_0 + L = G_0$, whence $2(g + G_0) = G_0$ for every $g \in G$. $\square$

We can now prove Theorem 2.

Proof of Theorem 2. We first show that there is at most one subgroup $L \in \mathcal{L}_G^*(S)$ with

$$|S + L| - |L| \le |S| - 1. \tag{28}$$

For a contradiction, assume that L, $L' \in \mathcal{L}_G^*(S)$ are distinct, L satisfies (28), and $|S + L'| - |L'| \le |S| - 1$. Find $G_0 \le G$ and $g_0 \in G_0$ such that (L1)–(L4) hold, and let $S_0 = S \cap (g_0 + L)$. It follows from Lemma 3 that $L' \le G_0$, whence

$$|L'| - 1 \ge |S + L'| - |S| \ge |S_0 + L'| - |S_0|. \tag{29}$$

Suppose that $L \not\leq L'$ and $L' \not\leq L$, and write $t = \varphi_{L'}(S_0)$; that is, t is the number of L'-cosets that intersect S_0. Since S_0 is not contained in a proper coset of L, and since $L \not\leq L'$, we have $t \geq 2$. Consequently, from $L' \not\leq L$ it follows that

$$|S_0 + L'| - |S_0| \geq t(|L'| - |L \cap L'|) \geq t|L'|/2 \geq |L'|,$$

contradicting (29). So we may assume either $L \leq L'$ or $L' \leq L$; switching the notation, if necessary, and recalling that $L' \neq L$, we assume that $L < L'$.

Since $L' \in \mathcal{L}^*_G(S)$, there exists a subgroup $G'_0 \leq G$, lying above L', and an element $g'_0 \in G'_0$ such that $|G'_0| \geq 4|L'|$, $(S + L') \setminus (g'_0 + L') = G \setminus G'_0$, and $(g'_0 + L') \cap S$ is not contained in a proper coset of L'. If $\varphi_{L'}(g'_0) = \varphi_{L'}(g_0)$, then $(g'_0 + L') \cap S = (g_0 + L') \cap S$, while, in view of $L' \leq G_0$, the right-hand side is contained in an L-coset, which, in view of $L < L'$, contradicts that $(g'_0 + L') \cap S$ is not contained in a proper coset of L'. Therefore, we conclude instead that $\varphi_{L'}(g_0) \neq \varphi_{L'}(g'_0)$. Thus, since $|\pi(\varphi_{L'}(S) \setminus \{\varphi_{L'}(g'_0)\})| = |\pi(G'_0/L')| \geq 4$, it follows from Proposition A that $|\pi(\varphi_{L'}(S) \setminus \{\varphi_{L'}(g_0)\})| = 1$, which is equivalent to

$$\pi((S + L') \setminus (g_0 + L')) = L'.$$

Hence, since $L < L' \leq G_0$, so that $(S + L') \setminus (g_0 + L') = G \setminus G_0$, it follows that $L' = G_0$, whence $S + L' = S + G_0 = G$, contradicting the assumption $L' \in \mathcal{L}^*_G(S)$. This establishes uniqueness of $L \in \mathcal{L}^*_G(S)$ satisfying (28).

Clearly, Lemma 5 implies assertion (ii) of Theorem 2, and therefore it remains to establish assertion (i). To this end, suppose that $L \in \mathcal{L}^*_G(S)$ satisfies (28), and that G_0 and g_0 are as in (L1)–(L4). We will show that $\eta_G(S) \geq |S|$ and $\kappa(\mathrm{Cay}^+_G(S)) = \lambda_G(S) = \lambda^*_G(S) = |S + L| - |L|$.

Suppose that there exists $H \in \mathcal{H}_G(S)$ with

$$|S + H| - |H| \leq |S| - 1. \tag{30}$$

Then $H \leq G_0$ by Lemma 3. If $H \leq L$, then from $(S + 2 * G) \cap H \neq \varnothing$ we obtain $(S + 2 * G) \cap L \neq \varnothing$, contradicting (L1)–(L4). Therefore $H \not\leq L$.

Let $S_0 = (g_0 + L) \cap S$, and denote by t the number of H-cosets intersecting S_0. In view of (30), and taking into account $H \leq G_0$ and $H \not\leq L$, we obtain

$$|H| - 1 \geq |S + H| - |S| \geq |S_0 + H| - |S_0| \geq t(|H| - |H \cap L|) \geq t|H|/2.$$

Hence $t = 1$. Thus, since S_0 is not contained in a coset of a proper subgroup of L, we conclude that $L \leq H$. Consequently, from (L1)–(L3) we get $2 * (G/H) = 2 * (G_0/H)$, and thus, in view of $(S + 2 * G) \cap H \neq \varnothing$ and taking into account (L4), we have

$$\varnothing \neq \varphi_H(S) \cap 2 * (G/H) = \varphi_H(S) \cap 2 * (G_0/H) = \{\varphi_H(g_0)\} \cap 2 * (G_0/H). \tag{31}$$

Since $\varphi_L(g_0)$ generates G_0/L, it follows from $H \geq L$ that $\varphi_H(g_0)$ generates the cyclic 2-group G_0/H. Thus (31) implies that $H = G_0$, whence $S + H = S + G_0 = G$, a contradiction. So we conclude that there are no subgroups $H \in \mathcal{H}_G(S)$ satisfying (30); that is, $\eta_G(S) \geq |S|$. Thus it follows by Lemma 5 that

$$\kappa(\mathrm{Cay}^+_G(S)) = \min\{\lambda^*_G(S), |S|\}. \tag{32}$$

The uniqueness of L, established above, implies that $\lambda^*_G(S) = |S + L| - |L|$, and now (28) shows that

$$\kappa(\mathrm{Cay}^+_G(S)) \leq \lambda_G(S) \leq \lambda^*_G(S) = |S + L| - |L| \leq |S| - 1.$$

Comparing this with (32), we see that, indeed, the first two inequalities are actually equalities. □

Finally, we prove Theorem 3.

Proof of Theorem 3. By Theorem 2, we have $\kappa(\mathrm{Cay}^+_G(S)) = |S + L| - |L|$ with a subgroup $L \leq G$, belonging to either $\mathcal{H}_G(S)$ or $\mathcal{L}^*_G(S)$. Let $F \leq G$ be a subgroup that minimizes $|S + F| - |F|$ over all subgroups with $S + F \neq G$. Assuming that

$$|S + F| - |F| < |S + L| - |L| \leq |S| - 1, \tag{33}$$

we will obtain a contradiction; evidently, this will prove the assertion.

¿From Lemma 2 and (33), it follows that either $S + F + L = S + L$ or $S + F + L = S + F$; in either case,

$$S + F + L \neq G. \tag{34}$$

Suppose first that $|L| \leq |F|$. Then Lemma 2 yields $S + F + L = S + F$, and thus

$$|S + F + L| - |F + L| = |S + F| - |F + L|.$$

The minimality of F now implies that $|F + L| = |F|$, whence $L \leq F$. If $L \in \mathcal{H}_G(S)$, then it follows in view of $L \leq F$ and $S + F \neq G$ that $F \in \mathcal{H}_G(S)$, implying $\kappa(\mathrm{Cay}^+_G(S)) \leq |S + F| - |F|$. However, since $\kappa(\mathrm{Cay}^+_G(S)) = |S + L| - |L|$, this contradicts (33). Therefore we may assume $L \in \mathcal{L}^*_G(S)$. Let G_0 be the subgroup from the definition of $\mathcal{L}^*_G(S)$. By Lemma 3 we then have $L \leq F \leq G_0$, whence

$$|S + F| = |G \setminus G_0| + |F| = (|S + L| - |L|) + |F|,$$

which contradicts (33) once more.

Next, suppose that $|F| \leq |L|$. Thus it follows by Lemma 2 that $S + L = S + F + L$. Hence

$$|S + F + L| - |F + L| = |S + L| - |F + L|. \tag{35}$$

If $L \in \mathcal{H}_G(S)$, then it follows in view of $L \leq F + L$ and (34) that $F + L \in \mathcal{H}_G(S)$; now (35) and the minimality of L give $|F + L| = |L|$, leading to $F \leq L$. We proceed to show that this holds in the case $L \in \mathcal{L}^*_G(S)$ as well. In this case, in view of (35) and (33), Lemma 3 gives $F + L \le G_0$, where G_0 is the subgroup from the definition of $\mathcal{L}^*_G(S)$. Thus (as in the previous paragraph)

$$|S + F + L| = |G \setminus G_0| + |F + L| = (|S + L| - |L|) + |F + L|.$$

Hence, since $|S + F + L| = |S + L|$, we obtain $|F + L| = |L|$, and therefore $F \le L$, as desired.

We have just shown that $F \le L$ holds true in either case. Consequently, from $|S + L| - |L| < |S| \le |S + F|$ and divisibility considerations, it follows that indeed $|S + L| - |L| \le |S + F| - |F|$, contradicting (33) and completing the proof. □

References

[A] N. Alon, Large sets in finite fields are sumsets, *J. Number Theory*, to appear.

[CGW03] B. Cheyne, V. Gupta, and C. Wheeler, Hamilton Cycles in Addition Graphs, *Rose-Hulman Undergraduate Math. Journal* **1** (4) (2003) (electronic).

[C92] F.R.K. Chung, Diameters and eigenvalues, *J. Amer. Math. Soc.* **2** (2) (1989), 187–196.

[Gr05] B.J. Green, Counting sets with small sumset, and the clique number of random Cayley graphs, *Combinatorica* **25** (2005), 307–326.

[Gk01] D.J. Grynkiewicz, Quasi-periodic decompositions and the Kemperman structure theorem, *European Journal of Combinatorics* **26** (5) (2005), 559–575.

[Gk02] ———, Sumsets, Zero-Sums and Extremal Combinatorics, *Ph.D. Dissertation*, Caltech (2005).

[Km60] J.H.B. Kemperman, On small subsets in an abelian group, *Acta Mathematica* **103** (1960), 63–88.

[Kn53] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 459–484.

[Kn55] ———, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.* **61** (1955), 429–434.

[L05] V.F. Lev, Critical pairs in abelian groups and Kemperman's structure theorem, *Internation Journal of Number Theory* **2** (3) (2006), 379–396.

[L] ———, Sums and differences along Hamiltonian cycles, *Submitted*.

[Mn76] H.B. Mann, Addition theorems: the addition theorems of group theory and number theory. Reprint, with corrections, of the 1965 original. Robert E. Krieger Publishing Co., Huntington, N.Y., 1976.

[Mr83] D. Marušič, Hamiltonian circuits in Cayley graphs, *Discrete Math.* **46** (1) (1983), 49–54.

Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, Campus Nord Edifici C3, Jordi Girona Salgado 1-3, Barcelona, Catalonia E-08034, Spain.

E-mail address: diambri@hotmail.com

Department of Mathematics, University of Haifa at Oranim, Tivon 36006, Israel

E-mail address: seva@math.haifa.ac.il

Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, Campus Nord Edifici C3, Jordi Girona Salgado 1-3, Barcelona, Catalonia E-08034, Spain

E-mail address: oserra@ma4.upc.edu