Diplomarbeit

Additive Combinatorics, Addition Cayley Graphs and Hamiltonicity

Angefertigt am
Mathematischen Institut

Vorgelegt der
Mathematisch-Naturwissenschaftlichen Fakultät der
Rheinischen Friedrich-Wilhelms-Universität Bonn

Mai 2012

Von

Jesse Beisegel

Aus
Bonn

Acknowledgements

I would like to thank everybody who helped in the course of this work.

In particular, I would like to thank Professor Saxena for bringing my attention to this subject and for his patience and generous support throughout.

Kurzfassung

Ein Additions-Cayley-Graph ist ein Graph, dessen Knotenmenge eine abelsche Gruppe ist, und der eine Kante zwischen zwei Knoten besitzt, wenn die Summe dieser Knoten in einer gegebenen Untermenge $S \subseteq G$ enthalten ist.

Trotz dieser intuitiven Konstruktion und ihrer engen Verwandtschaft zu den weit verbreiteten normalen Cayley-Graphen, wurden Additions-Cayley-Graphen bisher nur wenig untersucht: Nur etwa zehn Publikationen behandeln diese, unter einer Vielzahl von Namen.

Wegen ihrer Konstruktion über abelsche Gruppen und dem impliziten Gebrauch von Summenmengen (engl. sumsets) scheinen Additions-Cayley-Graphen ein hervorragendes Instrument zur Verwendung in der Additiven Kombinatorik zu sein. Diese Arbeit wird eine mögliche Verbindung dieser beiden Konzepte anstreben.

Kapitel 1 enthält eine kurze Einleitung zu einigen Grundlagen Additiver Kombinatorik. Die dort bewiesenen Aussagen werden in den übrigen Kapiteln benötigt, werden aber hier benutzt um die Methoden der Additiven Kombinatorik zu erläutern.

Da Additions-Cayley-Graphen eine Variante der üblichen Cayley-Graphen darstellen, möchten wir untersuchen, inwiefern sich diese - vor Allem in Bezug auf Additive Kombinatorik - unterscheiden.

In Kapitel 2 werden wir daher einige Eigenschaften von Cayley-Graphen präsentieren. Außerdem werden wir uns mit einem interessanten neuen Resultat über die Expander-Eigenschaften von Cayley Graphen beschäftigen, welches 2008 von Gamburd und Bourgain unter Zuhilfenahme von Methoden aus der Additiven Kombinatorik bewiesen wurde.

In Kapitel 3 widmen wir uns dem zentralen Thema dieser Arbeit: dem Additions-Cayley-Graphen. Wir werden begründen, wieso Additions-Cayley-Graphen ein nützliches graphentheoretisches Werkzeug der Additiven Kombinatorik darstellen, das in Lage ist Informationen aus der Graphentheorie auf Summenmengen und ähnliche Objekt zu übertragen. In diesem Sinne präsentieren wir zwei Resultate: Eines von B. Green, welches Methoden der Additiven Kombinatorik verwendet, um die Cliquenzahl von Additions-Cayley-Graphen zu berechnen, und ein anderes von N. Alon, welches die Unabhängigkeitszahl von Additions-Cayley-Graphen benutzt um die Größe bestimmter Summenmenge zu determinieren. Wir werden begründen, warum es gerade diese wechselseitige Beziehung ist, die Additions-Cayley-Graphen von normalen Cayley-Graphen mit Blick auf Additive Kombinatorik unterscheidet.

Da Additions-Cayley-Graphen nur verstreut in der Literatur zu finden sind, wurden viele ihrer Eigenschaften entweder gar nicht, oder nur unzureichend studiert. Eine dieser Eigenschaften ist die Hamiltonizität. Es ist eine bekannte Frage, ob Cayley-Graphen Hamilton-Kreise besitzen. Viele Publikationen sind zu diesem Thema erschienen, für Additions-Cayley-Graphen gibt es jedoch nur zwei, die sich mit diesem Thema auseinan-

dersetzen [CGW03, Lev10].

In Kapitel 4 werden wir diese Frage sowohl für Cayley-Graphen, als auch für Additions-Cayley-Graphen darlegen, und uns dann mit einer Vermutung beschäftigen, die Hamilton-Kreise für alle Additions-Cayley-Graphen über endliche zyklische Gruppen und Untermengen S von Kardinalität mindestens 4 postuliert.

Im letzten Abschnitt werden wir einige neue Resultate beweisen, welche Hamilton-Pfade für eine große Klasse von Additions-Cayley-Graphen liefern. Diese Pfade werden daraufhin benutzt, um zu argumentieren, dass die oben genannte Vermutung zu Untermengen S von Kardinalität mindestens 3 verbessert werden kann, wenn $|G| \equiv 1 \mod 4$.

Contents

Introduction

An addition Cayley graph is a graph whose vertex set is an abelian group G, and which has an edge between two vertices when the sum of these vertices is in a given subset of G, namely S.

In spite of their very intuitive construction and their closely related well-known pendant, the Cayley graph, these graphs have been subject to very little investigation. In fact they are mentioned only in about ten publications under a variety of different names.

Because of their definition over an abelian group and the implicit use of sumsets, addition Cayley graphs seem an ideal tool for additive combinatorics. Therefore, this work will investigate possible links between these two concepts.

Chapter 1 is a short introduction to some of the basic definitions and instruments of additive combinatorics. Here we will present some of the statements used in following chapters, and thus try to convey a few of the methods used in additive combinatorics.

As addition Cayley graphs are a variation of Cayley graphs, it is interesting to see in which way they differ from another, and to compare their relative use in additive combinatorics.

Chapter 2 will therefore introduce Cayley graphs and list some of their properties. We will also present a very interesting new result on Cayley graphs, namely a conclusive expander-property that was given by Gamburd and Bourgain in 2008 [BG08], and which makes strong use of additive combinatorics.

In Chapter 3, we will turn to our primary field of interest: the addition Cayley graph. After a formal introduction, we will suggest that addition Cayley graphs constitute an interesting graph theoretical tool in additive combinatorics, capable of transferring graph theoretical results to statements about sumsets and similar objects. To this end, we present two results: One by B. Green, which uses techniques from additive combinatorics to prove a result on the clique number of addition Cayley graphs [Gre05], and another result by N. Alon, which uses the independence number of an addition Cayley graph to give an estimation on particular sumsets [Alo07]. We will suggest that exactly this cross-reference distinguishes addition Cayley graphs from the regular Cayley graphs with regard to additive combinatorics.

As addition Cayley graphs have attained only sparse mention in the literature, many of their properties have not been properly examined. One of these is Hamiltonicity. It is a well-known question whether regular Cayley graphs are Hamiltonian and many papers have been published concerning this. For addition Cayley graphs, on the other hand, there are only two papers concerned with this subject [CGW03, Lev10].

In Chapter 4, after illustrating this problem for both addition Cayley graphs and regular Cayley graphs, we will deal with a conjecture that proposes Hamiltonicity for all addition Cayley graphs over finite cyclic groups and set S of cardinality at least 4.

In the last section we will prove some new results which yield Hamiltonian paths for a large class of addition Cayley graphs over cyclic groups. We will then use these Hamiltonian paths to motivate that the above mentioned conjecture can be improved to sets S of cardinality at least three, if $|G| \equiv 1 \mod 4$.

1 Additive Combinatorics

The theory of additive combinatorics is a rather new and rapidly expanding field of mathematics. Based on the work of mathematicians such as Szmerédi and Rusza in the 1970's, this area slowly developed, attracting the interest of many notable mathematicians, among them three Fields medallists: Jean Bourgain, Timothy Gowers and Terence Tao.

From the 1990's up until now, many important results have been found, most famously new proofs of Szemerédi's Theorem (for example by T. Gowers [Gow01]), a generalisation of Szemerédi's Theorem by T. Tao and B. Green [GT08] and the Sum-Product Theorem for Finite Fields ([BT04], [Kon03]).

The main objects of interest in additive combinatorics are additive sets and in particular their "additive structure".

An additive set is a pair (A, Z), where Z is an additive group and A a subset of Z. To explain the meaning of the term "additive structure", we will need to make the following definitions:

Definition 1.1. (sumset) Let A, B be additive sets in an ambient group Z. Then:

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

Definition 1.2. (difference set) Let A, B be additive sets in an ambient group Z. Then:

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

Definition 1.3. (iterated sumset) Let A be an additive set in an ambient group Z, $k \in \mathbb{Z}_+$. Then:

$$kA := \{a_1 + ... + a_k : a_1, ..., a_k\}$$

Definition 1.4. (dilation) Let A be an additive set in an ambient group Z, $k \in \mathbb{Z}_+$. Then:

$$k \cdot A := \{ka : a \in A\}$$

T. Tao and V. Vu [TV06] now give an informal criterion for a set A having additive structure. The following statements are all criteria for additive structure, which turn out to be "essentially equivalent" [TV06]:

- $A + A$ is small
- $A - A$ is small

- $A - A$ can be covered by a small number of translates of A
- kA is small for any fixed k
- there are many quadruples $(a_1, a_2, a_3, a_4) \in A \times A \times A \times A$ such that $a_1 + a_2 = a_3 + a_4$
- there are many quadruples $(a_1, a_2, a_3, a_4) \in A \times A \times A \times A$ such that $a_1 - a_2 = a_3 - a_4$

In the following, we will give a short introduction to additive combinatorics, giving the basic definitions and explaining some of the tools used in this field. A comprehensive overview of additive combinatorics can be found in [TV06].

We will also prove some of the lemmas and theorems, needed in the following, to illustrate the use of the presented tools.

1.1 Sum Estimates

Our first job will be to give precise definitions to the properties listed above.

We will say that $A + A$ ($A - A$) is small if its doubling constant (difference constant) is small:

Definition 1.5. (doubling constant) For an additive set A, the *doubling constant* $\sigma[A]$ is defined to be the quantity:

$$\sigma[A] := \frac{|A + A|}{|A|}$$

The *difference constant* $\delta[A]$ is defined as:

$$\delta[A] := \frac{|A - A|}{|A|}$$

As we are also interested in sums between two different sets, we will need a slightly modified version of the above:

Definition 1.6. (Rusza distance) Let A and B be two additive sets with a common ambient group Z. We define the *Rusza distance* $d(A, B)$ between these two sets to be the quantity:

$$d(A, B) := \log \frac{|A - B|}{|A|^{\frac{1}{2}} |B|^{\frac{1}{2}}}$$

In many ways the Ruzsa distance behaves like a metric, in particular it fulfils the triangle inequality:

Lemma 1.7. *[TV06] (Ruzsa triangle inequality) The Ruzsa distance $d(A, B)$ is non-negative, symmetric, and obeys the triangle inequality*

$$d(A, C) \leq d(A, B) + d(B, C)$$

for all additive sets A, B, C with common ambient group Z.

Proof. The Ruzsa distance is non-negative because:

$$\max(|A|, |B|) \leq |A - B|,$$

and symmetric because:

$$B - A = -(A - B).$$

Proving the triangle inequality we have:

$$a - c = (a - b) + (b - c).$$

Therefore we see that every element $a - c \in A - C$ has at least $|B|$ distinct representations of the form $x + y$ with $(x, y) \in (A - B) \times (B - C)$, implying that:

$$|A - C| \leq \frac{|A - B||B - C|}{|B|}.$$

This in turn yields the triangle inequality.

□

The only axiom of a metric not fulfilled by the Ruzsa distance is:

$$d(A, A) = 0 \Leftrightarrow A = A.$$

The other interesting value that arises between two additive sets is the additive energy which was already implicitly mentioned in the introduction:

Definition 1.8. (additive energy) Let A and B be two additive sets with common ambient group Z. We define the *additive energy* $E(A, B)$ between A and B to be the quantity:

$$E(A, B) := |\{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}|$$

Proposition 1.9. *[TV06] Let A, B be additive sets with ambient group Z. Then we have the identities:*

i) $|A||B| = \sum_{x \in A+B} |A \cap (x - B)|$,

ii) $E(A, B) = \sum_{x \in A+B} |A \cap (x - B)|^2 = \sum_{y \in A-B} |A \cap (B + y)|^2$.

Proof. i) This is proved by the following:

$$|A||B| = \sum_{x \in A+B} |\{(a, b) \in A \times B : a + b = x\}| = \sum_{x \in A+B} |A \cap (x + B)|.$$

ii) We can prove this with a simple equation:

$$\begin{aligned}\sum_{x\in A+B}|A\cap(x-B)|^2 &= \sum_{x\in A+B}|\{(a,b)\in A\times B : a+b=x\}|^2\\ &= \sum_{x\in A+B}\left|\left\{(a,a',b,b')\in A\times A\times B\times B : a+b=a'+b'=x\right\}\right|\\ &= \left|\left\{(a,a',b,b')\in A\times A\times B\times B : a+b=a'+b'\right\}\right| = E(A,B).\end{aligned}$$

□

This proposition shows us that the additive energy effectively counts the intersections of A with translates of B and $-B$, thus giving us a clue of how large $A+B$ and $A-B$ are going to be.

Before introducing approximate groups we need this lemma which will be useful throughout:

Lemma 1.10. *[TV06](Ruzsa's covering lemma) For any additive sets A, B with common ambient group G there exists an additive set $X \subseteq B$ with:*

- $B \subseteq A - A + X$;
- $|X| \leq \frac{|A+B|}{|A|}$;
- $|A + X| = |A||X|$;

Proof. We choose a set $X \subseteq$ such that $\{A + x : x \in X\}$ is a maximal disjoint sub-family of $\{A + b : b \in B\}$. Each of these $A + x$ has cardinality $|A|$ and is contained in $A + B$.

Therefore the cardinality of X must be less than $\frac{|A+B|}{|A|}$. As we have a maximal disjoint sub-family we also get $|A + X| = |A||X|$.

Now let $b \in B$. As our sub-family is maximal, $A + b$ must intersect $A + x$ for some $x \in X$. Thus b is an element of $A-A+x$. Since b was arbitrary, we have $B \subseteq A-A+X$.

□

Definition 1.11. (approximate group) Let $K \geq 1$. An additive set H is said to be a *K-approximate group* if it is symmetric ($H = -H$), contains the origin and $H + H$ can be covered by at most K translates of H.

The importance of approximate groups stems from this proposition:

Proposition 1.12. *[TV06] Let A be an additive set and let $K \geq 1$. Then the following statements are equivalent up to constants:*

- $\sigma[A] \leq K^{C_1}$;
- $|nA - mA| \leq K^{C_2(n+m)}|A|$;

- *there exists a K^{C_3}-approximate group H such that $A \subseteq x + H$ for all $x \in A$, and furthermore $|A| \geq K^{-C_3}|H|$.*

If B is in the same ambient group as A, then the following two statements are also equivalent up to constants:

- $d(A, B) \leq C_1 \log(K)$*;*
- *there exists a K^{C_2}-approximate group H such that $A \subseteq H + a$ and $B \subseteq H + b$ for all $a \in A$, $b \in B$, and furthermore $|A|$, $|B| \geq K^{-C_2}|H|$.*

As we only state this proposition to clarify the importance of approximate groups, we will not give a proof here, but refer to [TV06].

Essentially, this proposition implies that everything we have seen so far can also be interpreted in terms of approximate groups; sumset estimates are nothing other than estimates of specific approximate groups.

This proves to be very helpful, as it is possible to classify approximate groups in a similar manner to normal finite groups. However, this goes beyond the scope of this work and we must again refer to [TV06].

1.2 The Balog-Szemerédi-Gowers Theorem

The Balog-Szemerédi-Gowers Theorem is very important and used throughout additive combinatorics, but what makes it especially interesting in this context is the fact that its proof is entirely graph-theoretical.

To state the theorem we will first need to define partial sumsets:

Definition 1.13. (partial sumset) If A, B are additive sets with common ambient group Z and G is a subset of $A \times B$ we define the *partial sumset* to be:

$$A \overset{G}{+} B := \{a + b : (a, b) \in G\}$$

and the *partial difference set*:

$$A \overset{G}{-} B := \{a - b : (a, b) \in G\}$$

Supposing we have information about a partial sumset between two additive sets A and B, we want to be able to use this information for our estimation of the actual sumset $A + B$.

The Balog-Szemerédi-Gowers Theorem lets us do just that, although it will be necessary to slightly modify A and B.

Theorem 1.14. *(Balog-Szemerédi-Gowers theorem)[TV06]*

Let A, B be additive sets in an ambient group Z, and let $G \subseteq A \times B$ such that:

$$|G| \geq |A||B|/K \text{ and } |A \overset{G}{+} B| \leq K'|A|^{1/2}|B|^{1/2},$$

for some $K \geq 1$ and $K' > 0$. Then there exist subsets $A' \subseteq A$, $B' \subseteq B$ such that

$$|A'| \geq \frac{|A|}{4\sqrt{2}K}$$
$$|B'| \geq \frac{|B|}{4K}$$
$$|A' + B'| \leq 2^{12} K^4 (K')^3 |A|^{\frac{1}{2}} |B|^{\frac{1}{2}}$$

In particular we have

$$d(A', -B') \leq 5\log(K) + 3\log(K') + \mathcal{O}(1)$$

Looking back on the definition of partial sumsets, we can see that a graph-theoretical approach to this problem is quite natural, as G can be viewed as a bipartite graph with partitioned vertex set $A \cup B$ and edge set G.

We will try to count elements $a + b$ with $a \in A$ and $b \in B$ by excluding multiple representations of $a + b$ of the form:

$$a + b = \underbrace{(a + b')}_{x} - \underbrace{(a' + b')}_{y} + \underbrace{(a' + b)}_{z}.$$

If $x, y, z \in G$ we can identify this triple with a path of length three in our graph construction.

So our first task will be to count the number of paths of length three. We will do this by first counting the number of length two paths, and then extending these to paths of length three:

Lemma 1.15. *(paths of length two)[TV06] Let $\mathcal{G}$ be a bipartite graph with vertex set $V(\mathcal{G}) = A \cup B$ and edge set $E(\mathcal{G})$, with $|E(\mathcal{G})| \geq \frac{|A||B|}{K}$ for some $K \geq 1$. Then, for any $0 < \epsilon < 1$, there exists a subset $A' \subseteq A$ such that*

$$|A'| \geq \frac{|A|}{\sqrt{2}K}$$

and such that at least $(1 - \epsilon)$ of the pairs of vertices $a, a' \in A'$ are connected by at least $\frac{\epsilon}{2K^2}|B|$ paths of length two in $\mathcal{G}$.

Proof. By decreasing K if necessary we may assume $|E(\mathcal{G})| = \frac{|A||B|}{K}$. Using some combinatorial identities and Cauchy-Schwarz we get:

$$\mathbb{E}_{a,a' \in A} \frac{|N(a) \cap N(a')|}{|B|} \geq \frac{1}{K^2}$$

Let Ω be the set of all pairs such that a, a' are not connected by at least $\frac{\epsilon}{2K^2}|B|$ paths of length two, i.e. $|N(a) \cap N(a')| < \frac{\epsilon}{2K^2}|B|$. This leads to:

$$\mathbb{E}_{a,a' \in A} \mathbb{I}((a,a') \in \Omega) \frac{|N(a) \cap N(a')|}{|B|} < \frac{\epsilon}{2K^2}.$$

If we rearrange this equation and use the pigeon-hole principle we get the following:

$$\frac{1}{|A|^2} \sum_{a,a' \in N(b)} \left(1 - \frac{1}{\epsilon} \mathbb{I}((a,a') \in \Omega)\right) \geq \frac{1}{2K^2}.$$

Now let $A' := N(b)$. Thus $|A'| \geq \frac{|A|}{|\sqrt{2}K|}$ and $|\{a, a' \in A' : (a,a') \in \Omega\}| \leq \epsilon |A'|^2$

□

Lemma 1.16. *(paths of length three)[TV06] Let $\mathcal{G}$ be a bipartite graph with vertex set $V(\mathcal{G}) = A \cup B$ and edge set $E(\mathcal{G})$ with $|E(\mathcal{G})| \geq \frac{|A||B|}{K}$ for some $K \geq 1$. Then there exist $A' \subseteq A$, $B' \subseteq B$ with $|A|' \geq \frac{|A|}{4\sqrt{2}K}$ and $|B'| \geq \frac{|B|}{4K}$, such that every $a \in A'$ and $b \in B'$ is connected by at least $\frac{|A||B|}{2^{12}K^4}$ paths of length three.*

Proof. To prove this lemma we will first apply Lemma 1.15 to get paths of length two. Then we will choose some of these paths and extend them by one edge.

To apply Lemma 1.15 we need to reduce our graph to an induced subgraph, by only using those vertices of A that have degree at least $\frac{|B|}{2K}$. We can use Lemma 1.15 to get a set A^* of size:

$$|A^*| \geq \frac{|A|}{2\sqrt{2}K},$$

such that $1 - \frac{1}{16K}$ of the pairs $a, a' \in A^*$ are connected by at least $\frac{C|B|}{128K^3}$ paths of length two, where C is a constant that derives from constructing the induced subgraph.

We delete vertices from A^* such that at least $\left(1 - \frac{1}{8K}\right)$ pairs are connected by at least $\frac{L^2|B|}{8K^2}$ paths of length two, to get a set A' of size:

$$|A'| \geq \frac{|A|}{4\sqrt{2}K}.$$

Now we only need to construct a $B' \subseteq B$ such that all demands of the statement are met:

$$B' := \left\{ b \in B : |\{a \in A^* : (a,b) \in E\}| \geq \frac{|A^*|}{4K} \right\}$$

By some easy counting arguments we can see that this set has the right size.

If we pick an $a \in A'$ and a $b \in B'$ we can see that, by construction, b is adjacent to at least $\frac{|A^*|}{4K}$ elements of A^* of which at least half are connected to a by at least $\frac{L^2|B|}{8K^2}$ paths of length two. Altogether we have at least:

$$\frac{|A||B|}{2^{12}K^4}$$

paths of length three.

□

Now that we have a bound for the paths of length three we can use this in the manner implied in the beginning of this section:

Proof of Theorem 1.14. We can assume that A and B are disjoint, as this can be achieved by modifying the ambient group. Let $\mathcal{G}$ be a graph with vertex set $V(\mathcal{G}) := A \cup B$ and edge set G. Using Lemma 1.16 we can find A', B' such that $|A'| \geq \frac{|A|}{4\sqrt{2}K}$, $|B'| \geq \frac{|B|}{4K}$ and every pair $a \in A'$, $b \in B'$ is connected by at least $\frac{|A||B|}{2^1 2K^4}$ paths of length three:

$$|\{(a', b') \in A \times B : (a, b'), (a', b'), (a', b) \in G\}| \geq \frac{|A||B|}{2^{12}K^4}.$$

By:

$$a + b = \underbrace{(a + b')}_{x} - \underbrace{(a' + b')}_{y} + \underbrace{(a' + b)}_{z},$$

we can conclude that:

$$|\{(x, y, z) : x, y, z \in A \overset{\mathrm{G}}{+} B, x - y + z = a + b\}| \geq \frac{|A||B|}{2^{12}K^4}. \tag{1.1}$$

The total amount of triples (x,y,z) is bounded by:

$$|A \overset{\mathrm{G}}{+} B|^3 \leq (K')^3 |A|^{\frac{3}{2}} |B|^{\frac{3}{2}}.$$

By dividing the right side of this inequality with the right side of 1.1 and thus eliminating some of the multiple representations, we get:

$$|A' + B'| \leq 2^{12} K^4 (K')^3 |A|^{\frac{1}{2}} |B|^{\frac{1}{2}}.$$

□

If in practice there is difficulty in gaining any information even on the partial sumset, the following proposition (which we will be needing later on) enables us to use the additive energy between A and B to receive an estimate on a partial sumset.

Proposition 1.17. *[TV06] Let A, B be additive sets in an ambient group Z. Then, supposing:*

$$E(A, B) \geq \frac{|A|^{\frac{3}{2}} |B|^{\frac{3}{2}}}{K}$$

for some $K \geq 1$, then there exists $G \subseteq A \times B$ such that:

$$|G| \geq \frac{|A||B|}{2K} \text{ and } |A \overset{G}{+} B| \geq 2K |A^{\frac{1}{2}}||B|^{\frac{1}{2}}.$$

Proof. We set S to be:

$$S := \left\{ x \in A + B : |A \cap (x - B)| \geq \frac{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}{2K} \right\}.$$

This definition leads to the following:

$$\frac{|S||A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}{2K} \leq \sum_{x \in S} |A \cap (x - B)| \leq |A||B|,$$

where the second inequality is implied by Proposition 1.9.

Now we can define the subset G that we are looking for:

$$G := \{(a, b) \in A \times B : a + b \in S\}.$$

Using the above inequalities, it is easy to show that G fulfils all the necessary properties.

□

1.3 Product Estimates

Up until now, we have been working with additive sets in commutative ambient groups. Some of the results we have found can even be transposed into a non-commutative setting.

In Chapter 1 we will rely heavily on product estimates as we will be dealing with Cayley Graphs which are not necessarily defined over commutative groups. Most of the results at the end of this section are prerequisites for Chapter 2 which are only proved in this section to highlight the use of the concepts presented here.

We begin by defining the product set:

Definition 1.18. (product set) Let A, B be multiplicative sets in an ambient group G. Then:

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

Definition 1.19. (inverse set) Let A be a multiplicative set. Then:

$$A^{-1} := \{a^{-1} : a \in A\}$$

Definition 1.20. (iterated product set) Let A be a multiplicative set. Then:

$$A^{\cdot n} := A \cdot ... \cdot A \text{ for } n \geq 1. \ A^{\cdot 0} := \{1\} \text{ and } A^{\cdot -n} := (A^{\cdot n})^{-1} = (A^{-1})^{\cdot n}$$

One obvious drawback in the non-commutative setting is the fact that, in general, $A \cdot B$ and $B \cdot A$ will be very different sets with completely different cardinalities.

The first manifestation of this fact arises with the non-commutative equivalent of the Ruzsa distance, which will not be symmetric.

Thus we will have two different distances between the sets A and B, the left-invariant Ruzsa distance $d(A,B)$ and the right-invariant Ruzsa distance $d^*(A^{-1},B^{-1})$.

It is standard to use the left-invariant version, which from now on, will be called the Ruzsa distance and which is defined as follows:

Definition 1.21. ((left-invariant) Ruzsa distance) Let A, B be multiplicative sets in an ambient group Z. Then:

$$d(A,B) := \log\left(\frac{|A\cdot B^{-1}|}{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}\right)$$

Again this obeys the triangle inequality:

Lemma 1.22. *((left-invariant) Ruzsa triangle inequality) The left-invariant Ruzsa distance obeys the triangle inequality*

$$d(A,C) \leq d(A,B) + d(B,C)$$

for all multiplicative sets A, B, C with common ambient group Z.

Proof. As in the commutative case in Lemma 1.7 we get:

$$|AC^{-1}| \leq \frac{|AB^{-1}||BC^{-1}|}{|B|},$$

which yields the desired triangle inequality.

□

There is also a non-commutative equivalent of the additive energy:

Definition 1.23. (multiplicative energy) Let A, B be multiplicative sets with ambient group Z. Then:

$$E(A,B) := \left|\{(a,a',b,b') \in A\times A\times B\times B : ab = a'b'\}\right|.$$

The properties of the multiplicative energy are not as strong as those of the additive energy. But an equivalent version of Proposition 1.9 exists, and from this we can deduce the following simple results, which are stated as an exercise in [TV06]:

Proposition 1.24. *If A and B are multiplicative sets in the same ambient group, then:*

i) $E(A,B) \geq \frac{|A|^2|B|^2}{|A\cdot B|}$,

ii) $E(A,A^{-1}) = E(A^{-1},A)$.

Proof. i) This is just an implication of Proposition 1.9 and the Cauchy-Schwarz inequality.

ii) For $a, a' \in A$ and $b, b' \in A^{-1}$ it is easy to see that $a \cdot b = a' \cdot b'$ if and only if $b \cdot (b')^{-1} = a^{-1}a'$. Therefore (a, a', b, b') is in the set underlying the definition of $E(A, A^{-1})$ if and only if $(b, a^{-1}, (b')^{-1}, a')$ is in the set underlying the definition of $E(A^{-1}, A)$, proving the equation.

□

Before introducing the K-approximate group, we will quickly state a non-commutative version of the Ruzsa covering lemma, which can be proved like the original:

Lemma 1.25. *[TV06](non-commutative version of the Ruzsa covering lemma) Let A, B be multiplicative sets in an ambient group G. Suppose that $|A \cdot B| \leq K|A|$. Then there exists a finite set $X \subseteq B$ of cardinality at most K, such that:*

$$B \subset A^{-1} \cdot A \cdot X.$$

Proof. The proof is again an analogue of the commutative case.

□

Definition 1.26. (multiplicative K -approximate group) Let $K \geq 1$. A multiplicative set H is said to be a *multiplicative K-approximate group* if it is symmetric, contains the identity, and is such that there is a set X of cardinality $|X| \leq K$ such that we have the inclusions:

i) $H \cdot H \subseteq X \cdot H \subseteq H \cdot X \cdot X$, and

ii) $H \cdot H \subseteq H \cdot X \subseteq X \cdot X \cdot H$

As in the commutative setting, approximate groups can be used as an alternative to describe product set estimates.

However, we must assume that $|A \cdot A \cdot A|$ is small to avoid complications:

Lemma 1.27. *[TV06] Let A be a multiplicative set in a group G, and let $K \geq 1$. Then the following statements are equivalent up to constants , in the sense that if the jth property holds for some absolute constant C_j, then the kth property will hold for some absolute constant C_k depending on C_j:*

i) $|A \cdot A \cdot A| \leq K^{C_1}|A|$;

ii) there exists a K^{C_2}*approximate group H containing A where* $|H| \leq K^{C_2}|A|$.

Proof. i) ⇒ ii)

We define our approximate group H to be $H' \cdot H' \cdot H'$ with $H' = A \cup \{1\} \cup A^{-1}$.

Using the Ruzsa triangle inequality and (i) we see that $|H| \leq K^{\mathcal{O}(1)}|A|$.

As H is obviously symmetric and as $A \subseteq H$ we only need to show the inclusions from 1.26. Again using the triangle inequality and (i) we see that $|H' \cdot H \cdot H| \leq K^{\mathcal{O}(1)}$. Thus using the Ruzsa covering lemma, we can find a set $Y \subset H \cdot H$ and $|Y| \leq K^{\mathcal{O}(1)}$ such that:

$$H \cdot H \subset H'^{-1} \cdot H' \cdot Y \subseteq H \cdot Y.$$

We embed Y in a symmetric set $X = Y \cup Y^{-1}$ to get:

$$H \cdot H \subseteq H \cdot X; H \cdot H \subset X \cdot H.$$

As $X \subset H \cdot H$:

$$H \cdot X \subset H \cdot H \cdot H \subset X \cdot H \cdot H \subset X \cdot X \cdot H.$$

ii) $\Rightarrow$ i)

To prove this direction, we need to use the second inclusion from the definition from 1.26:

$$|A \cdot A \cdot A| \leq |H \cdot H \cdot H| \leq |H \cdot H \cdot X| \leq |H \cdot X \cdot X| \leq |H||X|^2 \leq K^{C_2}|A||X|^2.$$

As $|X| \leq K^{C_2}$ there is a constant C_1 only dependent on C_2 such that this is less than $K^{C_1}|A|$.

□

We can also give an equivalent to Proposition 1.12:

Theorem 1.28. *[TV06] Let A, B be multiplicative sets in a group G, and let $K \geq 1$. Then the following statements are equivalent up to constants, in the sense that if the jth property holds for some absolute constant C_j, then the kth property will hold for some absolute constant C_k depending on C_j:*

i) $d(A, B) \leq C_1(1 + \log(K))$;

ii) there exists a $C_2K^{C_2}$-approximate group H such that $|H| \leq C_2K^{C_2}|A|$, $A \subset X \cdot H$ and $B \subset Y \cdot H$ for some multiplicative sets X, Y of cardinality at most $C_2K^{C_2}$.

For the proof of this theorem we need the following lemma. As the equivalent statement in [TV06] is faulty (mentioned in the errata), the author has modified the proof of Proposition 4.5 in [Tao08] such that it is comprehensible in this context.

Lemma 1.29. *[Tao08] Let A be multiplicative set such that $d(A, A) \leq \log(K)$ for some $K \geq 1$. Then there exists a symmetric set S such that $|S| \geq \frac{|A|}{2K}$ and:*

$$\left|A \cdot S^{\cdot n} \cdot A^{-1}\right| \leq 2^n K^{2n+1}|A|,$$

for all integers $n \geq 1$.

Proof. We define S as:

$$S := \left\{ x \in A^{-1} \times A : |A \cap (A \cdot x)| > \frac{|A|}{2K} \right\}.$$

From Proposition 1.9 and Proposition 1.24 we can deduce that:

$$\sum_{x \in A^{-1} \cdot A} |A \cap (A \cdot x)|^2 = E(A^{-1}, A) = E(A, A^{-1}) \geq \frac{|A|^4}{A \cdot A^{-1}} \geq \frac{|A|^3}{K},$$

and that:

$$\sum_{x \in A^{-1} \cdot A} |A \cap (A \cdot x)| = |A|^2.$$

Using these equations and bounding $|A \cap (A \cdot x)|$ with $|A|$ we get:

$$\frac{|A|}{2K} \leq |S|.$$

Let x be an arbitrary element of $A \cdot S^{\cdot n} \cdot A^{-1}$. We can write $x = a_0 s_1 \dots s_n b_{n+1}^{-1}$, where $s_1, \dots, s_n \in S$ and $a_0, b_{n+1} \in A$.

The value we will be interested in, is the cardinality of the following set:

$$Y := \left\{ (y_0, \dots, y_n) \in (A \cdot A^{-1})^{\times (n+1)} : y_0 \cdot \ldots \cdot y_n \in A \cdot S^{\cdot n} \cdot A^{-1} \right\}$$

Obviously, $|A \cdot A^{-1}|^{n+1}$ is an upper bound for this value.

For a lower bound, we need to take a look at a typical element x of $A \cdot S^{\cdot n} \cdot A^{-1}$. This can be written as:

$$x = a_0 s_1 \dots s_n b_{n+1}^{-1},$$

where $a_0, b_{n+1} \in A$ and $s_1, \dots, s_n \in S$.

We can expand x with arbitrary elements of the ambient group:

$$x = (a_0 c_1^{-1}) \cdot (c_1 s_1 c_2^{-1}) \dots \cdot (c_{n-1} s_{n-1} c_n^{-1}) \cdot (c_n s_n b_{n+1}),$$

where $c_1, \dots, c_n \in Z$.

For this to be a multiplication of $n+1$ elements of $A \cdot A^{-1}$, it is necessary that $c_1, \dots, c_n \in A$ and $c_1 s_1, \dots, c_n s_n \in A$. By the definition of S, this will be true in more than $\left(\frac{|A|}{2K}\right)^n$ cases, giving us a lower bound for the cardinality of Y of $|A \cdot S^{\cdot n} \cdot A^{-1}| \cdot \left(\frac{|A|}{2K}\right)^n$ and thus proving the statement.

□

Now we are able to prove Theorem 1.28:

Proof of Theorem 1.28. $(i) \Rightarrow (ii)$:

By (i) we can deduce that $d(A, A) = \mathcal{O}(\log K)$. Therefore we can apply Lemma 1.29 to A and get:

$$|A \cdot S^{\cdot 3} \cdot A^{-1}| \leq K^{\mathcal{O}(1)}|A|. \tag{1.2}$$

This implies that $|S^{\cdot 3}| \leq K^{\mathcal{O}(1)}|S|$ and because of Lemma 1.27 we can find a $\mathcal{O}(K^{\mathcal{O}(1)})$-approximate group H of size at most $K^{\mathcal{O}(1)}|A|$ containing S.

Equation 4.2 also implies that $|A \cdot S| \leq K^{\mathcal{O}(1)}|A|$ and thus $d(A, S) = \mathcal{O}(\log K)$. Because H is a approximate group containing S we see that $d(S, H^{-1})$ and the triangle inequality yields:

$$|A \cdot H| \leq K^{\mathcal{O}(1)}|A|.$$

Using this, we can apply the covering lemma to obtain a set Y of cardinality $K^{\mathcal{O}(1)}$ such that:

$$A \subset Y \cdot H \cdot H^{-1}. \tag{1.3}$$

As H is an approximate group, $H = H^{-1}$ and $H \cdot H \subset Z \cdot H$ for some set Z of size $K^{\mathcal{O}(1)}$. Thus, $A \subset (Y \cdot Z) \cdot H$, with $|Y \cdot Z| \leq K^{\mathcal{O}(1)}$.

The same property can be shown for B in an analogous way.

$(ii) \Rightarrow (i)$:

This implication is a direct result of Lemma 1.27.

□

The Balog-Szemerédi-Gowers theorem retains its whole strength in the non-commutative setting, as the proof is purely graph theoretical. It will be very important in Chapter 2, were we will use its corollaries to examine expander-properties of Cayley graphs.

Theorem 1.30. *(non-commutative version of the B-S-G theorem)[TV06]*

Let A, B be multiplicative sets in an ambient group Z and let $G \subseteq A \times B$ be such that:

$$|G| \geq \frac{|A||B|}{K} \text{ and } |A \overset{G}{\cdot} B| \leq K'|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$$

for some $K \geq 1$ and $K' \geq 0$. Then there exist subsets $A' \subseteq A$, $B' \subseteq B$ such that

$$|A'| \geq \frac{|A|}{4\sqrt{2}K},\ |B'| \geq \frac{|B|}{4K},\ |A' \cdot B'| \leq 2^{12}K^4(K')^3|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$$

In particular we have:

$$d(A', B'^{-1}) \leq 5\log(K) + 3\log(K') + \mathcal{O}(1)$$

Proof. This theorem can be proved exactly the same way as the abelian version of the BSG-Theorem, as the proof of that theorem was purely graph theoretical and did not make any use of the assumed commutativity of the ambient group.

□

As in the commutative case we have a link between the BSG-Theorem and the multiplicative energy:

Proposition 1.31. *[TV06] Let A, B be multiplicative sets in an ambient group Z. Then, supposing:*

$$E(A,B) \geq \frac{|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}}{K}$$

for some $K \geq 1$, then there exists $G \subseteq A \times B$ such that:

$$|G| \geq \frac{|A||B|}{2K} \text{ and } |A \overset{G}{\cdot} B| \geq 2K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}.$$

Proof. The proof of this proposition is analogue to the commutative case.

□

Corollary 1.32. *[TV06] Let A, B be multiplicative sets in an ambient group Z such that:*

$$E(A,B) \geq \frac{|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}}{K},$$

for some $K > 1$. Then there exists a subset $A' \subset A$ such that:

- $|A'| = \Omega(K^{-\mathcal{O}(1)}|A|)$
- $|A' \cdot (A')^{-1}| = \mathcal{O}\left(K^{\mathcal{O}(1)}|A|\right)$

for some absolute constant C.

Proof. As $E(A,B)$ meets the prerequisites of Proposition 1.31, we get a set $G \subseteq A \times B$ which lets us apply Theorem 1.30.

We receive A', B' with:

- $|A'| = \Omega\left(K^{\mathcal{O}(1)}|A|\right)$
- $|A' \cdot B'| \leq 2^{19}K^7|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$
- $d(A', B'^{-1}) \leq 8\log(2K)\mathcal{O}(1)$

Additionally we can use the triangle inequality of the Ruzsa-distance to get:

$$d(A', A') \leq d(A', B'^{-1}) + d(A', B'^{-1}) = 2d(A', B'^{-1})$$

Combining this, we get:

$$|A' \cdot (A')^{-1}| = \mathcal{O}\left(K^{\mathcal{O}(1)}|A|\right).$$

□

There are also some interesting product estimates that are restricted to particular groups.

A good example of such a theorem is the following:

Lemma 1.33. *[Hel08] Let H be a subset of $SL_2(\mathbb{F}_p)$. Assume that $|H| < p^{3-\delta}$ for $\delta > 0$ and that H is not contained in any proper subgroup of $SL_2(\mathbb{F}_p)$. Then:*

$$|H \cdot H \cdot H| > c|H|^{1+\kappa},$$

where $c > 0$ and $\kappa > 0$ depend only on δ.

The proof of this statement is very expansive and it will not be possible to present it in this setting. Therefore we will present only the first step, which acts as a guide to the further steps of the proof; in fact the following lemma already contains a very similar statement.

Definition 1.34. Given a positive integer r and a subset A of a group G. We define A_r to be the set of all products of at most r elements of $A \cup A^{-1}$:

$$A_r := \left\{ g_1 \cdot g_2 \cdot \ldots \cdot g_r : g_i \in A \cup A^{-1} \cup \{1\} \right\}.$$

Lemma 1.35. *[Hel08] Let $n > 2$ be an integer. Let A be a finite subset of a group G. Suppose that:*

$$|A_n| > c|A|^{1+\epsilon},$$

for some $c > 0$, $\epsilon > 0$. Then

$$|A \cdot A \cdot A| > c'|A|^{1+\epsilon'},$$

where $c' > 0$, $\epsilon' > 0$ depend only on c, ϵ.

Proof. Using the inequality received in the proof of Lemma 1.22:

$$|AC^{-1}| \leq \frac{|AB^{-1}||BC^{-1}|}{|B|} \tag{1.4}$$

we get the following:

$$\frac{|A_n|}{|A|} = \frac{|A_{n-2}A_2|}{|A|} \leq \frac{|A_{n-2}A^{-1}|}{|A|}\frac{|AA_2|}{|A|} \leq \frac{|A_{n-1}|}{|A|}\frac{|A_3|}{|A|}.$$

By induction on n this leads to:

$$\frac{|A_n|}{|A|} \leq \left(\frac{|A_3|}{|A|}^{n-2}\right).$$

Now we need to bound A_3 with a power of $A \cdot A \cdot A$. We can do this by bounding each combination of $|XYZ|$ where $XYZ \in \{A, A^{-1}\}$.

We will only bound two of these combinations here, the rest can be done easily by taking inverses and replacing A by A^{-1}.

Using equation 1.4 we get:

$$|AA^{-1}A||A| = |AAA^{-1}||A^{-1}| \leq |AAA||A^{-1}A^{-1}| \leq |AAA|^2,$$

and:

$$|AA^{-1}A||A| \leq |AA^{-1}A^{-1}||AA| = |AAA^{-1}||AA| \leq |AAA|^2|AAA|.$$

Now we can adjust c' and ϵ' depending only on c, ϵ and n to get the desired statement. □

Proving that $|A_n| > c|A|^{1+\epsilon}$ is very hard and uses discrete Fourier-analysis. Thus we must refer to [Hel08] for the rest of the proof.

Altogether, it can be said that while some of the results of additive combinatorics can be transferred to a commutative setting, statements tend to be slightly weaker and some results are missing completely. Many questions in this field are still open, and it is far from being as conclusive as the theory of the commutative case.

1.4 Freiman Homomorphisms

In group theory it is often necessary to transfer a certain property or problem from one group G to another group G'. We do this by using group homomorphisms.

Recall that:

Definition 1.36. (group homomorphism) Let G and G' be two groups. We call a map $\phi : G \to G'$ a *group homomorphism*, if:

i) ϕ maps the unit element of G onto the unit element of G',

ii) for all $g_1, g_2 \in G$ we have $\phi(g_1 + g_2) = \phi(g_1) + \phi(g_2)$.

If in addition there is an inverse map $\phi^{-1} : G' \to G$, which is a homomorphism, then we say that ϕ is an isomorphism.

As the group homomorphisms are a very powerful tool, we want a similar construction for additive sets. Group homomorphisms are not ideal with respect to additive sets; firstly, we are not dealing with an additively closed group, and secondly, criterion (ii) does not mirror any of the properties we have been interested in so far.

Therefore it is necessary to use a new construction, that of the Freiman homomorphism.

Definition 1.37. (Freiman homomorphism) Let $s \geq 1$ and let A, B be additive sets with ambient group Z and W respectively. A *Freiman homomorphism* ϕ, of order s, from (A, Z) to (B, W) is a map $\phi : A \to B$ with the property that:

$$a_1 + ... + a_s = a'_1 + ... + a'_s \Rightarrow \phi(a_1) + ... + \phi(a_s) = \phi(a'_1) + ... + \phi(a'_s),$$

for all $a_1, ..., a_s, a'_1, ..., a'_s \in A$. If in addition there is an inverse map $\phi^{-1} : B \to A$ which is a Freiman homomorphism of order s from (B, W) to (A, Z), then we say that ϕ is a *Freiman isomorphism* of order s, and that (A,Z) and (B,W) are Freiman isomorphic of order s. We write this as $(A, Z) \cong_s (B, W)$.

As an abbreviation we will sometimes denote a Freiman homomorphism of order s simply as an s-homomorphism and, as before, we will mostly drop the ambient group, writing A instead of (A, Z).

Comparing these two definitions, we see that the Freiman homomorphism is weaker than a group homomorphism. In fact, every group homomorphism can be turned into a Freiman homomorphism of arbitrary order by restriction.

Also every Freiman homomorphism of order k is also a Freiman homomorphism of order k', for all $k' < k$.

Example 1.38.

- As already mentioned, if $\phi : G \to G'$ is a group homomorphism, then it induces a Freiman homomorphism from (A, G) to $(\phi(A), G)$ of any order.
- If $x \in G$, then the translation map $\phi : G \to G$ defined by $\phi(g) := g + x$ is a Freiman homomorphism from (A, G) to $(A + x, G)$ of any order.
- The sets $\{0, 1, 10, 11\}$ and $\{0, 1, 100, 101\}$ are Freiman isomorphic of order k, for any $k < 10$, but not Freiman isomorphic of order k for any $k \geq 10$.

Proposition 1.39. *[TV06] Let (A, G) be an additive set, and let $\phi : (A, G) \to (\phi(A), H)$ be a surjective Freiman homomorphism of order k. Then we have:*

$$|\epsilon_1\phi(A_1) + \ldots + \epsilon_k\phi(A_k)| \leq |\epsilon_1 A_1 + \ldots + \epsilon_k A_k|,$$

whenever $A_1, \ldots, A_k$ are non-empty subsets of A and $\epsilon_1, \ldots, \epsilon_k = \pm 1$.

If ϕ is in fact a Freiman isomorphism of order k, then we may replace the inequality with equality. In particular, if A and B are Freiman isomorphic of order k, then:

$$|lB - mB| = |lA - mA|,$$

whenever $l, m \geq 0$ and $l + m \leq k$.

Proof. Define an equivalence relation $\backsim$ on $A_1 \times \ldots \times A_k$ by declaring:

$$(a_1, \ldots, a_k) \backsim (a'_1, \ldots, a'_k) \Leftrightarrow \epsilon_1 a_1 + \ldots \epsilon_k a_k = \epsilon_1 a'_1, \ldots \epsilon_k a'_k.$$

Rewriting the right-hand-side as:

$$\sum_{j:\epsilon_j=1} a_j + \sum_{j:\epsilon_j=-1} a'_j = \sum_{j:\epsilon_j=-1} a_j + \sum_{j:\epsilon_j=1} a'_j,$$

we can see that this equivalence relation is respected by a Freiman homomorphism of order k.

The number of equivalence classes in $A_1 \times \ldots \times A_k$ is:

$$|\epsilon_1 A_1 + \ldots + \epsilon_k A_k|.$$

Applying a Freiman k-homomorphism can only reduce the number of equivalence classes as it respects the relation; this proves the lemma.

□

This lemma shows that Freiman isomorphisms do exactly what we need them to do: preserve all relevant quantities (i.e. the cardinality of iterated sums and of difference sets, and also the doubling constant and the energy) from one additive set to another.

We will be using Freiman homomorphisms in Section 3.2 so we will prove some of the results needed for that section in this chapter, to illustrate the application of these objects.

We will start with a very simple result, and after defining the Freiman dimension go on to some more complex statements.

Proposition 1.40. *[Gre05] Suppose that $A \cong_6 B$. Then:*

i) $A + A \cong_3 B + B$ and

ii) any $C \subseteq A + A$ is 3-isomorphic to a subset of $B + B$. In particular we have $A\hat{+}A \cong_3 B\hat{+}B$.

Proof. i) As $A \cong_6 B$ there is a 6-isomorphism $\phi : A \to B$, i.e. a map, such that for any $a_1, \ldots, a_6, a'_1, \ldots, a'_6$ with:

$$a_1 + \ldots + a_6 = a'_1 + \ldots + a'_6$$

we have:

$$\phi(a_1) + \ldots + \phi(a_6) = \phi(a'_1) + \ldots \phi(a'_6).$$

Also as ϕ is a isomorphism, we get the same for ϕ^{-1}.

We now define a new map $\phi' : A + A \to B + B$ by:

$$\phi'(c) = \phi(a_1) + \phi(a_2),$$

where $a_1, a_2 \in A$, $c \in A + A$ and $c = a_1 + a_2$.

Suppose there are $a'_1, a'_2 \in A$ such that $a'_1 + a'_2 = c = a_1 + a_2$. Then, as ϕ is a 6-isomorphism, we have $\phi(a_1)+\phi(a_2) = \phi(a'_1)+\phi(a'_2)$. Therefore ϕ' is well-defined.

Let $c_1, c_2, c_3, c'_1, c'_2, c'_3 \in A + A$ such that:

$$c_1 + c_2 + c_3 = c'_1 + c'_2 + c'_3,$$

and $a_{11}, a_{12}, \ldots, a_{32}, a'_{11}, \ldots a'_{32}$ such that:

$$c_i = a_{i1} + a_{i2}$$

and

$$c'_i = a'_{i1} + a'_{i2},$$

for $i \in \{1, 2, 3\}$.

Then we get:

$$\begin{aligned}\phi'(c_1) + \phi'(c_2) + \phi'(c_3) = \phi'(a_{11}) + \ldots \phi'(a_{32}) &= \phi'(a'_{11}) + \ldots \phi'(a'_{32}) \\ &= \phi'(c'_1) + \phi'(c'_2) + \phi'(c'_3).\end{aligned}$$

This proves that ϕ' is a 3-homomorphism. It is an isomorphism, because ϕ is an isomorphism.

ii) This can be proven by restricting ϕ' to C.

□

Another result in this vein that we will need in the Chapter 3 is the following:

Lemma 1.41. *[Gre05] The number of s-isomorphism classes of subsets of a vector space W of size k is at most k^{2sk}.*

To prove this we need a statement about s-isomorphic sets in vector spaces.

Now let F be a field, $k \in \mathbb{Z}_+$ and W a vector space over F. Let V_k be a k-dimensional vector space over F with basis $\{e_1, \ldots, e_k\}$. For any sequence $\sigma := \{a_1, \ldots, a_k\}$ with $a_1, \ldots, a_k \in W$ define the linear map $\phi_\sigma : V_k \to W$ by:

$$\phi_\sigma \left(\sum \lambda_i e_i \right) = \sum \lambda_i e_i$$

For the following results we will need some notation:

Notation 1.42.

- We say that $v \in V$ is satisfied by σ if $v \in \ker \phi_\sigma$
- A vector of the form
$$e_{i_1} + \ldots + e_{i_s} - e_{j_1} - \ldots - e_{j_s}$$
is called an s-relation.
- Denote the set of all s-relations in V_k by $\mathcal{R}_s$.

Lemma 1.43. *[Gre05] Suppose that $\sigma = (a_i)_{i=1}^k$ and $\sigma' = (a'_i)_{i=1}^k$ are two sequences of distinct elements of W, and suppose that $Span\,(\mathcal{R}_s \cap \ker \phi_\sigma) = Span\,(\mathcal{R}_s \cap \ker \phi_{\sigma'})$. Then the sets $A = \{a_1, \ldots, a_k\}$ and $A' = \{a'_1, \ldots, a'_k\}$ are s-isomorphic.*

Proof. Because $\mathcal{R}_s \subseteq W$ and $\ker \phi_\sigma$ is a subspace of W, we get:

$$\mathcal{R}_s \cap Span\,(\mathcal{R}_s \cap \ker \phi_\sigma) = \mathcal{R}_s \cap \ker \phi_\sigma,$$

and thus:

$$\mathcal{R}_s \cap \ker \phi_\sigma = \mathcal{R}_s \cap \ker \phi_{\sigma'}.$$

Due to this fact the map $\psi : A \to A'$ with $a_i \mapsto a'_i$ is an isomorphism.

□

Proof of Lemma 3.22. Let $A = \{a_1, \ldots, a_k\}$ be a subset of W and $\sigma := (a_1, \ldots, a_k)$. By Lemma 1.43 we know that the number of s-isomorphism classes A is at most the number of subspaces of V_k spanned by s-relations. There are at most k^{2s} s-relations in V_k, and for reasons of dimension any subspace of V_k is spanned by at most k of these.

□

Up until now, we have talked about additive sets as the tuple of an ambient group and a subset of this group, without specifying what these ambient groups are and whether it is important which one we use.

The same set can have many different ambient groups, and the choice of an ambient group can greatly influence on the properties of such a set:

Example 1.44. [TV06] The additive sets $(\{1,2,3\}, \mathbb{Z}_7))$, $(\{1,2,3\}, \mathbb{Z}_6))$ and $(\{1,2,3\}, \mathbb{Z}))$ are all Freiman isomorphic of order 2.

The same set $\{1,2,3\}$ in another ambient group, $(\{1,2,3\}, \mathbb{Z}_3))$, however is not Freiman isomorphic to the above additive sets and has a different additive structure.

To simplify we will introduce the concept of the universal ambient group, which will fix an ambient group up to a k-isomorphism:

Definition 1.45. (universal ambient group) Let (A, G) be an additive set and let the order k of the Freiman homomorphism be fixed.

We say that G is a *universal ambient group* (of order k) for the additive set A, if every Freiman homomorphism $\phi : (A, G) \to (B, H)$ has a unique extension to a group-homomorphism $\phi_{ext} : G \to H$.

Using this definition, we can say that an additive group G' is a universal ambient group for (A, G) if there exists an additive set (A', G') which is Freiman isomorphic to (A, G) such that G' is a universal ambient group for A'; we then call (A', G') an embedding of (A, G) inside the ambient group G'.

With this in mind we are equipped to introduce the Freiman dimension:

Definition 1.46. (Freiman dimension) Let A be an additive set. We define the *Freiman dimension* of A to be the unique non-negative integer $r_Z A = d$ such that $G/\operatorname{Tor}(G)$ is group isomorphic to $\mathbb{Z}^{d+1}$ for every universal ambient group G of A.

The Freiman dimension is dependent on the order of the Freiman homomorphism used for the universal ambient group (see Definition 1.45).

We have given the definition of the Freiman dimension a very general form which will not be very useful in practice. As we will only need the Freiman dimension of vector spaces W over a field F, we give an equivalent definition, which holds only in this case:

Definition 1.47. Let W be a vector space over the field F and $A \subseteq W$. Then the *Freiman dimension* of A is:

$$r_F(A) = \dim \mathrm{Hom}_2(A, F) - 1,$$

where $\mathrm{Hom}_s(A, W')$ is the vector space of Freiman s-homomorphisms $\phi : A \to W'$, for a vector space W'.

Using this definition, it is easy to see that:

$$\dim \mathrm{Hom}_2(A, W') = (r_F(A))^{\dim W'}. \tag{1.5}$$

The statement we want to present in this context is:

Theorem 1.48. *[Gre05] Let W and W' be finite-dimensional vector spaces over a field F and let $A \subseteq W$ be a finite non-empty set of Freiman dimension $r := r_F(A)$.*
Then there is a subset $\{a_1, \ldots, a_{r+1}\} \subseteq A$ with the following properties:

i) For any $w'_1, \ldots, w'_{r+1} \in W'$ there is a unique $\phi \in \mathrm{Hom}_2(A, W')$ with $\phi(a_i) = w'_i$ for $i = 1, \ldots, r+1$.

ii) If $w'_1, \ldots, w'_{r+1}$ from (i) are linearly independent, then ϕ is an isomorphism.

iii) If $a \in A$ then there are $\lambda_1, \ldots, \lambda_{r+1} \in F$ (depending only on a) with:

$$\lambda_1 + \ldots + \lambda_{r+1} = 1_F \text{ and}$$

$$\phi(a) = \lambda_1\phi(a_1) + \ldots + \lambda_{r+1}\phi(a_{r+1}), \text{ for any } \phi \in \mathrm{Hom}_2(A, W').$$

However, first we will have to show this basic result on maps in general:

Lemma 1.49. *[Gre05] Let F be a field and let A be a finite non-empty set. By Ψ we denote the vector space of all maps from A to F and by Φ a subspace of Ψ.*
If $d = \dim \Phi$, then there exists a subset $\{a_1, \ldots, a_d\} \subseteq A$ with the following properties:

i) For any $f_1, \ldots, f_d \in F$ there is a unique $\phi \in \Phi$ with $\phi(a_i) = f_i$, for all $i \in \{1, \ldots, d\}$;

ii) If $a \in A$ then there are $\lambda_1, \ldots, \lambda_d \in F$ (depending only on a) such that:

$$\phi(a) = \lambda_1\phi(a_1) + \ldots + \lambda_d(a_d),$$

for any $\phi \in \Phi$.

If the constant map, which sends everything in A to $\mathbb{1}_F$, lies in Φ then we may assume that $\lambda_1 + \ldots + \lambda_d = 1$.

Proof. i) Let $A = \{a_1, \ldots, a_k\}$. As a basis for Ψ we can choose the set $\{\alpha_1, \ldots, \alpha_k\}$, where α_i is the map defined by $\alpha_i(a_j) = \delta_{ij}$.

As Φ has dimension d, we can find $k - d$ of the α_i which together with Φ span Ψ. By relabelling we can assume the following:

$$\Psi = \Phi \oplus \mathrm{Span}(\alpha_{d+1}, \ldots, \alpha_k). \tag{1.6}$$

Therefore for any $f_1, \ldots, f_d \in F$ there are $\phi \in \Phi$ and $e_{d+1}, \ldots, e_k \in F$ such that:

$$f_1\alpha_1 + \ldots + f_d\alpha_d = \phi + e_{d+1}\alpha_{d+1} + \ldots + e_k\alpha_k,$$

and thus $\phi(a_i) = f_i$, for all $i \in \{1, \ldots, d\}$. ϕ is unique because we have a direct sum in 1.6.

ii) Let $t_x(\phi) : \Phi \to F$ be a linear functional such that $t_x(\phi) = \phi(x)$. As the space of linear functionals from Φ to F has dimension d, $t_a, t_{a_1}, \ldots, t_{a_d}$ are linearly dependent for a fixed a. Thus we can find $\mu, \mu_1, \ldots, \mu_d \in F$, not all zero, such that:

$$\mu t_a(\phi) + \mu_1 t_{a_1}(\phi) + \ldots + \mu_d t_{a_d}(\phi) = 0, \tag{1.7}$$

for any $\phi \in \Phi$.

If μ were zero, we would get a contradiction to (i). Thus we have the wanted equation with $\lambda_i = -\mu^{-1}\mu_i$.

Suppose the constant map lies in Φ. Then 1.7 implies that:

$$\lambda_1 + \ldots \lambda_d = 1.$$

□

Now we have the necessary instruments to prove Theorem 1.48

Proof of Theorem 1.48. As we have:

$$\mathrm{Hom}_2(A, F^n) \cong (\mathrm{Hom}_2(A, F))^n,$$

we can prove (i) and (iii) by applying Lemma 1.49.

For (ii) suppose that $\phi \in \mathrm{Hom}_2(A, W')$ is not an isomorphism, i.e. that there are $b_1, b_2, b_3, b_4 \in A$ such that:

$$\phi(b_1) + \phi(b_2) = \phi(b_3) + \phi(b_4) \text{ and } b_1 + b_2 \neq b_3 + b_4$$

By the previous part we get $\lambda_{1_i}, \lambda_{2_i}, \lambda_{3_i}, \lambda_{4_i} \in F$, for b_1, b_2, b_3, b_4 respectively, such that:

$$\psi(b_1) + \psi(b_2) - \psi(b_3) - \psi(b_4) = \sum_{i=1}^{r+1} (\lambda_{1_i} + \lambda_{2_i} - \lambda_{3_i} - \lambda_{4_i})\, \psi(a_i),$$

for all vector spaces V over F and all $\psi \in \mathrm{Hom}_2(A, V)$. As $b_1 + b_2 - b_3 - b_4 \neq 0$, by setting V to W and ψ to id we see that not all the $(\lambda_{1_i} + \lambda_{2_i} - \lambda_{3_i} - \lambda_{4_i})$ are equal to zero.

So, let $\psi = \phi$ and $V = W'$. We then see that $\phi(a_1) = w'_1, \ldots, \phi(a_{r+1}) = w'_{r+1}$ is linearly dependent.

□

2 Cayley Graphs and Expanders

2.1 Cayley Graphs

Cayley graphs were employed for the first time by Arthur Cayley in 1878 to visualize groups. Both Dehn, in 1911, and Schreier, in 1927, noticed that the concept of Cayley graphs could be used for more than mere visualization, using it to prove results in algebra.

Since then Cayley graphs have undergone several waves of interest. In 1969 the Lovasz conjecture, stating that every connected vertex transitive graph contains a Hamiltonian path [Lov70], renewed the attraction of Cayley graphs.

Soon it was conjectured that every connected Cayley graph with three or more vertices is Hamiltonian [GM05].

This conjecture resulted in many publications proving Hamiltonicity for different types of groups, the full conjectures though (both the Lovasz conjecture and the above) are still open.

The next wave of interest came with the advent of expanders in the 1970's. In fact, the first construction of an explicit family of expander graphs by Margulis [Mar73] is implicitly derived from Cayley graphs on $SL_3(p)$ of 3×3 matrices with determinant 1 over $\mathbb{F}_p$ [HLW06].

Since then many Cayley graphs have been shown to be expanders, for example some Cayley graphs on $SL_2(p)$ in [Lub94] or more recently in [BG08].

In this chapter we will concentrate on the expander properties of Cayley graphs. We will begin with a formal definition of a Cayley graph:

Definition 2.1. (Cayley graph) Let G be a finite group and S a subset of G such that $e \notin S$ and for every $s \in S$ we have $s^{-1} \in S$.

Then the *Cayley graph* induced by S on G, $Cay(G, S)$, is the graph with vertex set G and edge set $E(Cay(G, S)) := \{\{x, y\} : xy^{-1} \in S\}$

Remark 2.2. The following properties of Cayley graphs can be shown very easily:

- Every Cayley graph $Cay(G, S)$ is $|S|$-regular
- Cayley graphs are vertex transitive
- A Cayley graph is connected if and only if S generates the group G

Definition 2.3. (adjacency matrix) Let $\mathcal{G}$ be a graph and $|\mathcal{G}| = n$. The *adjacency matrix* of $\mathcal{G}$, $A(\mathcal{G})$, is a $|\mathcal{G}| \times |\mathcal{G}|$ matrix with rows and columns indexed by the vertices of $\mathcal{G}$, such that the i, j entry is 1 if and only if $\{i, j\} \in E(\mathcal{G})$.

With $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{n-1}$ we shall denote the eigenvalues of of the adjacency matrix $A(\mathcal{G})$ in descending order.

The set of eigenvalues of $A(\mathcal{G})$, $\{\lambda_0, \lambda_1, \ldots, \lambda_{n-1}\}$ is called the *spectrum* of $\mathcal{G}$. The value $\lambda_0 - \lambda_1$ is called the *spectral gap*.

The adjacency matrix of an undirected graph is symmetric. Therefore all the eigenvalues are real.

Further on we will be interested in the eigenvalues of Cayley graphs and addition Cayley graphs. For this purpose we need to introduce characters:

Definition 2.4. (character) A *character* of a group G is a homomorphism $\chi : G \to \mathbb{C}^*$.

Our use of characters will only be very superficial. Therefore we will not delve too far into this rather complicated subject, but instead state some necessary properties:

Remark 2.5. Characters of groups have the following simple properties:

- The trivial character maps all elements of G to 1.
- Because χ is a homomorphism we have $\chi(gh) = \chi(g)\chi(h)$ for all $g, h \in G$.
- If G is the cyclic group $\mathbb{Z}_n$ we have:

  $$\chi_k(g) = e^{\frac{2\pi ikh}{n}},$$

  for $g \in G$.

Using characters we can completely describe the eigenvalues of Cayley graphs (but whether they can be efficiently calculated is dependent on the group):

Lemma 2.6. *[HLW06] Let $\hat{A}$ be the normalized adjacency matrix of the Cayley graph $Cay(G, S)$ and χ a character of G. Then the vector $(\chi(h))_{h \in G}$ is an eigenvector of $\hat{A}$, with eigenvalue:*

$$\frac{1}{|S|} \cdot \sum_{s \in S} \chi(s),$$

and the trivial character corresponds to the trivial eigenvalue.

Proof. This can be proved in the following way:

$$\left(\hat{A} \cdot \chi\right)(h) = \frac{1}{|S|} \sum_{s \in S} (\chi(h)\chi(s)) = \frac{1}{|S|} \left(\sum_{s \in S} \chi(s)\right) \cdot \chi(h).$$

□

2.2 Expanders

Cayley graphs have many interesting properties. One of these is that they can be used to construct families of expander graphs.

Roughly, an expander is a graph which is both sparse and highly connected. There are many ways to characterise expanders and in this section we want to introduce two of these: the standard characterisation, and an algebraic variant.

Expanders are an important tool in many fields of mathematics, but also in computer science and physics. For example, they are used to construct communication networks, for error-correcting codes and also to create pseudo-randomness.

As mentioned, one way to construct expanders is to use Cayley graphs, in fact the first construction of an explicit family of expander graphs [Mar73] used methods derived from Cayley graphs on the groups $SL_3(p)$ [HLW06].

In 1994 a similar construction for $SL_2(p)$ was found by Lubotzky [Lub94]. In the next section we will explain this in more detail, as the result which we want to present will be an improvement on this construction, which was made by Bourgain an Gamburd in 2008 [BG08] using methods from additive combinatorics.

In the following we will give a short introduction to expanders and explain the connection between these and Cayley graphs. A more thorough introduction to this field can be found in a paper by Hoory, Linial and Widgerson [HLW06].

From now on in this section, all graphs will be d-regular.

To give an explicit definition of expanders, we first have to define the expansion ratio:

Definition 2.7. (expansion ratio) Let $\mathcal{G}$ be a graph. The *expansion ratio* of $\mathcal{G}$ is defined as:

$$c(\mathcal{G}) := \min_{\{S:|S|\leq\frac{n}{2}\}} \frac{|\delta S|}{|S|}$$

The expansion ratio is also sometimes called the *expansion* of $\mathcal{G}$.

Obviously we now want to examine the size of $c(\mathcal{G})$ for a given graph $\mathcal{G}$, or for a family of graphs $\{\mathcal{G}_{i\in\mathbb{N}}\}$.

In particular, it will be of interest whether the expansion ratio can be zero. If we can exclude this for a whole family of graphs, then we have a family of expanders:

Definition 2.8. (family of expanders) A sequence of d-regular graphs $\{\mathcal{G}\}_{i\in\mathbb{N}}$ of size increasing with i is a *family of expander graphs* if there exists $\epsilon > 0$ with:

$$c\left(\mathcal{G}_i\right) > \epsilon, \text{ for all } i.$$

Sometimes it is useful to know whether the expansion ratio of a family of expanders is larger or equal than a given constant C. Then we speak of a family of C-expanders:

Definition 2.9. (C-expander) A family of d-regular graphs $\mathcal{G}_{n,d}$ forms a *family of C-expanders* if there is a fixed positive constant C, such that:

$$\liminf_{n\to\infty} c(\mathcal{G}_{n,d}) \geq C$$

Now we are able to give some examples of expanders:

Example 2.10. We let $\{\mathcal{G}_{i\in\mathbb{N}}\}$ be a family of expanders with:

- $V(\mathcal{G}_i) := \mathbb{Z}_i \times \mathbb{Z}_i$;
- $d = 8$;
- every vertex (x, y) has edges to: $(x + y, y)$, $(x - y, y)$, $(x, y + x)$, $(x, y - x)$ and $(x + y + 1, y)$, $(x - y + 1, y)$, $(x, y + x + 1)$, $(x, y - x + 1)$.

Example 2.11. We let $\{\mathcal{G}_{p\in\mathbb{N}}\}$, p prime, be a family of expanders with:

- $V(\mathcal{G}_p) := \mathbb{Z}_p$;
- $d = 3$;
- every vertex x has edges to $x + 1$, $x - 1$ and x^{-1}, where $0^{-1} := 0$ (Figure 2.1).

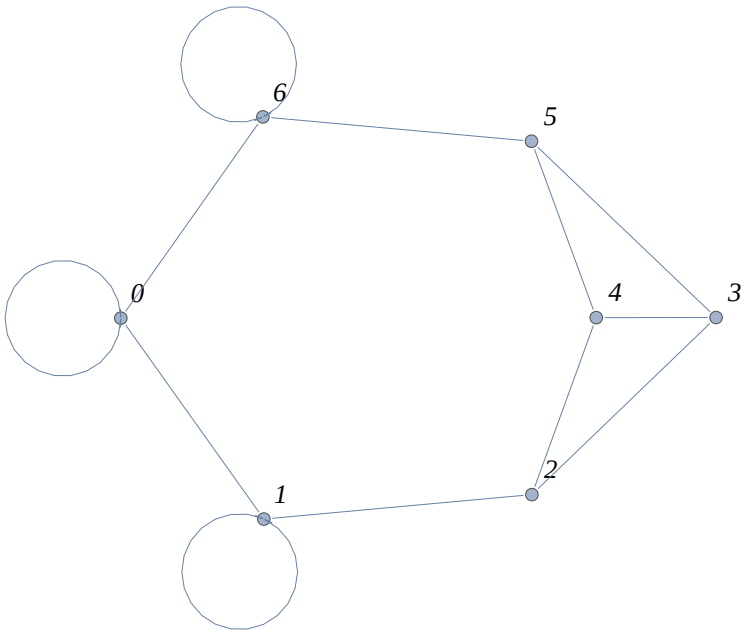


Figure 2.1: $\mathcal{G}_7$

With these definitions in mind, we can now progress to give an algebraic definition of expander graphs. To do this we will use the spectrum of $\mathcal{G}$, i.e. the eigenvalues of $A(\mathcal{G})$, defined in the last section.

As already mentioned, it will be of interest to describe the size of $c(\mathcal{G})$ and using the spectrum of $\mathcal{G}$, we can give first upper and lower bounds:

Theorem 2.12. *[Dod84, AM85, Alo86] Let $\mathcal{G}$ be a d-regular graph. Then:*

$$\frac{d-\lambda_1}{2} \geq c(\mathcal{G}) \geq \sqrt{2d(d-\lambda_1)}$$

Using this theorem, we can formulate an algebraic expansion criterion, as the expansion of $\mathcal{G}$ can only be zero, if $d = \lambda_1$. Thus we have:

Definition 2.13. (family of expanders, algebraic version) A family of graphs $\mathcal{G}_i$ forms a family of C-expanders if:

$$\limsup_{i\to\infty} \lambda_1(A(\mathcal{G}_i)) < d,$$

where λ_1 denotes the second largest eigenvalue of the adjacency matrix $A(\mathcal{G}_i)$.
We call $d - \lambda_1$ the *spectral gap*.

We can see that by determining or bounding the spectral gap, we can also bound the expansion ratio from both sides.

In the following we will present some bounds for the spectral gap. The first will be the Expander Mixing Lemma:

Definition 2.14. ($E(S,T)$) Let $\mathcal{G}$ be a graph. For $S, T \subset V(\mathcal{G})$ we denote the set of edges from S to T, by:

$$E(S,T) := \{\{u,v\} : u \in S, v \in T, \{u,v\} \in E(\mathcal{G})\}$$

Definition 2.15. Let $\mathcal{G}$ be a graph and let $\{\lambda_0, \ldots, \lambda_{n-1}\}$ be its spectrum. Then $\lambda := \max(\lambda_1, \lambda_{n-1})$.

Lemma 2.16. *(expander mixing lemma)[HLW06] Let $\mathcal{G}$ be a d-regular graph with n vertices and let $\lambda := \max(\lambda_1, \lambda_{n-1})$. Then for all $S, T \subseteq V(\mathcal{G})$:*

$$\left| |E(S,T)| - \frac{d|S||T|}{n} \right| \leq \lambda\sqrt{|S||T|}.$$

As defined above $|E(S,T)|$ is the number of edges between S and T. On the other hand, $\frac{d|S||T|}{n}$ denotes the expected number of edges between S and T in a random graph.

Thus when λ is small, i.e. the spectral gap large, the number of edges between S and T in $\mathcal{G}$ is very similar to that of a random graph.

Proof of Lemma 2.16. We begin with some notation:

Let A denote the adjacency matrix of $\mathcal{G}$. Then $\lambda_0, \ldots, \lambda_{n-1}$ are the eigenvalues in order of their size and $v_0, \ldots, v_{n-1}$ respective eigenvectors that form an orthonormal basis. $\mathbb{1}_S$ and $\mathbb{1}_T$ are the characteristic vectors of S and T respectively, i.e. the vectors that are 1, if a vertex is in S (respectively T) and zero otherwise.

We can represent these vectors with the above basis: $\mathbb{1}_S = \sum_{i=0}^{n-1} \alpha_i v_i$, $\mathbb{1}_T = \sum_{i=0}^{n-1} \beta_i v_i$

Now we have:

$$|E(S,T)| = \mathbb{1}_S A \mathbb{1}_T = \sum_{i=0}^{n-1} \alpha_i v_i A \sum_{i=0}^{n-1} \beta_i v_i.$$

Using the fact that $\{v_i\}_i$ is an orthonormal basis of eigenvectors we get:

$$\sum_{i=0}^{n-1} \lambda_i \alpha_i \beta_i.$$

We know from Section 2.1 that $v_0 = \frac{1}{\sqrt{n}}\mathbb{1}$ and $\lambda_0 = d$, because $\mathcal{G}$ is d-regular. Therefore $\alpha_0 = \left\langle \mathbb{1}_S, \frac{1}{\sqrt{n}}\mathbb{1} \right\rangle = \frac{|S|}{\sqrt{n}}$ and $\beta_0 = \left\langle \mathbb{1}_T, \frac{1}{\sqrt{n}}\mathbb{1} \right\rangle = \frac{|T|}{\sqrt{n}}$. So we get:

$$|E(S,T)| = d\frac{|S||T|}{n} + \sum_{i=1}^{n-1} \lambda_i \alpha_i \beta_i.$$

Finally we can use the definition of λ and Cauchy-Schwarz to get our result:

$$\begin{aligned}\left| |E(S,T)| - d\frac{|S||T|}{n} \right| = \left| \sum_{i=1}^{n-1} \lambda_i \alpha_i \beta_i \right| &\leq \lambda \sum_{i=1}^{n-1} |\alpha_i \beta_i| \leq \lambda \left\|\alpha\right\|_2 \left\|\beta\right\|_2 \\ &= \lambda \left\|\mathbb{1}_S\right\|_2 \left\|\mathbb{1}_T\right\|_2 = \lambda\sqrt{|S||T|}.\end{aligned}$$

□

As we have seen, the spectrum of a graph is critical for its expander properties. Hence the following concept is very useful in the theory of expansion:

Definition 2.17. ((n,d,λ)-graph) A (n,d,λ)-*graph* is a d-regular graph on n vertices, in which the absolute value of each non-trivial eigenvalue of its adjacency matrix is at most λ.

An upper bound for the spectral gap was given by Alon, Boppana, Nilli, and Friedmann:

Theorem 2.18. *[Nil91, Fri93] There exists a constant c, such that for every d-regular graph $\mathcal{G}$ with $|V(\mathcal{G})| = n$ and diameter Δ:*

$$\lambda_1 \geq 2\sqrt{d-1} \cdot \left(1 - \frac{c}{\Delta^2}\right).$$

2.3 Expander Properties of Cayley Graphs over $SL_2(\mathbb{Z})$

Let S be a subset of $SL_2(\mathbb{Z})$. Then by using the natural projection of S modulo p (p being an arbitrary prime number), i.e., S_p, we can generate a Cayley graph: $Cay(SL_2(\mathbb{F}_p), S_p)$.

The question to be answered in this section is whether these Cayley graphs are expanders.

In [Lub95] Lubotzky formulated this question in a slightly different manner, as the 1-2-3 question:

Problem 2.19. Let $p \geq 5$ be a prime. Define

$$S_p^1 := \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

$$S_p^2 := \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\}$$

$$S_p^2 := \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \right\}$$

and let $\mathcal{G}_p^i := Cay(SL_2(\mathbb{F}_p), S_p^i)$, for $i \in \{1, 2, 3\}$. The question is whether any of the $\mathcal{G}_p^i$ form a family of expanders.

As $\langle S^1 \rangle$ and $\langle S^2 \rangle$ have finite index in $SL_2(\mathbb{Z})$, $\mathcal{G}_p^1$ and $\mathcal{G}_p^2$ are families of expanders as $p \to \infty$ (this is shown in Theorem 4.3.2 of [Lub94]).

$\langle S^3 \rangle$ on the other hand, has infinite index and is thus not covered by [Lub94]. So the question remains whether $\mathcal{G}_p^3$ is a family of expanders.

Fortunately, it was resolved in a recent result by Bourgain and Gamburd [BG08], who give a necessary and sufficient criterion for S, such that $Cay(SL_2(\mathbb{F}_p), S_p)$ forms a family of expanders:

Theorem 2.20. *[BG08] Let S be a set of elements in $SL_2(\mathbb{Z})$. Then the the Cayley graphs $Cay(SL_2(\mathbb{F}_p), S_p)$ form a family of expanders if and only if $\langle S \rangle$ is non-elementary, i.e. the limit set of $\langle S \rangle$ consists of more than two points (equivalently $\langle S \rangle$ does not contain a solvable subgroup of finite index).*

This theorem is a result of Theorem 2.21 stated below.

Theorem 2.21. *[BG08] Fix $k \geq 2$ and suppose that $S_p = \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$ is a symmetric generating set for $SL_2(\mathbb{F}_p)$ such that:*

$$\text{girth}(Cay(SL_2(\mathbb{F}_p), S_p)) \geq \tau \log_{2k}(p),$$

where τ is a fixed constant independent of p.
Then the Cayley graphs $Cay(SL_2(\mathbb{F}_p), S_p)$ form a family of expanders.

A large part of the proof of this theorem uses additive combinatorics. Therefore, as we are particularly interested in the connection between additive combinatorics and Cayley graphs, we will present the part of the proof using additive combinatorics in detail, while sketching the rest of the proof to give an idea how the result is achieved.

Proof of Theorem 2.21. To prove this theorem we need to show two things:

- We need to show that all the non-trivial eigenvalues of $A(SL_2(Cay(\mathbb{F}_p)), S_p)$ appear with a high multiplicity, and
- We need to give an upper bound of the number of short closed cycles, i.e. the number of returns to identity for random walks of length of order $\log(|SL_2(\mathbb{F}_p)|)$.

We will begin by bounding the number of short closed cycles.

To find an upper bound of the short closed cycles, we will use methods from additive combinatorics. As we are dealing with sets which are not necessarily commutative, we will use some of the non-commutative product set estimates which were presented in Chapter 1.

While proving spectral gap results (and thus results on expanders) in the above way was already used in [SX91] in 1991, the idea of using additive combinatorics in this context is novel to the paper by Bourgain and Gamburd ([BG08]) presented in this section.

By W_{2l} we denote the number of closed walks from identity to itself of length $2l$. It will now be our aim to bound this value.

First we need to define the following probability measure :

Definition 2.22. Let G be a group and $S \subseteq G$ a generating set. Then we define μ_S as:

$$\mu_S(x) := \frac{1}{|S|} \sum_{g \in S} \delta_g(x),$$

where

$$\delta_g(x) := \begin{cases} 1, & \text{if } x = g, \\ 0, & \text{if } x \neq g; \end{cases}$$

We let $\mu^{(l)}$ denote:

$$\mu^{(l)} := \underbrace{\mu * \cdots * \mu}_{l}$$

where:

$$\mu * \nu(x) := \sum_{g \in G} \mu(xg^{-1})\nu(g).$$

And we define $\|\nu\|_2$ and $\|\nu\|_\infty$ as:

$$\|\nu\|_2 := \left(\sum_{g \in G} \nu^2(g) \right)^{\frac{1}{2}},$$

and

$$\|\nu\|_\infty := \max_{g\in G} \nu(g).$$

With this notation in mind, we need to examine the value $\mu_{S_p}^{(2l)}(1)$. By writing this expression out and comparing it to the definition of the Cayley graph, we can see that this value effectively counts the number of closed walks from identity to itself, the δ-operator checking if the necessary edges are in place. Thus we get the following equation:

$$\mu_{S_p}^{(2l)}(1) = \frac{W_{2l}}{(2k)^{2l}}$$

Now we can reduce searching for a bound of closed walks from identity to itself to bounding the probability $\mu_{S_p}^{(2l)}(1)$:

Lemma 2.23. *[BG08] Suppose $\mathcal{G}\left(SL_2(\mathbb{F}_p), S_p\right)$ with $|S_p| = 2k$ satisfies:*

$$\text{girth}(\mathcal{G}\left(SL_2(\mathbb{F}_p), S_p\right)) \geq \tau \log_{2k}(p).$$

Then for any $\epsilon > 0$ there is $C(\epsilon, \tau)$ such that for $l > C(\epsilon, \tau)\log_{2k}(p)$:

$$\left\|\mu_{S_p}^{(l)}\right\|_2 < p^{-\frac{3}{2}+\epsilon}.$$

Before we prove this lemma we will finish the proof of Theorem 2.21.
We have:

$$\mu_{S_p}^{(2l)}(1) = \sum_{g\in G} \mu^{(l)}(g)\mu^{(l)}(g^{-1}) = \sum_{g\in G} \left(\mu^{(l)}(g)\right)^2 = \left\|\mu^{(l)}\right\|_2^2,$$

as S_p is a symmetric generating set.
We can use the bound obtained in Lemma 2.23:

$$W_{2l} = \mu_{S_p}^{(2l)}(1)(2k)^{2l} < \frac{(2k^{2l})}{p^{3-2\epsilon}}.$$

Let $N = |SL_2(\mathbb{F}_p)|$. It can be shown that for p large enough S_p generates all of $SL_2(\mathbb{F}_p)$, implying that $Cay(SL_2(\mathbb{F}_p), S_p)$ is connected. Therefore we can write the eigenvalues of the adjacency matrix A as:

$$2k = \lambda_0 > \lambda_1 \geq \ldots \geq \lambda_{N-1} \geq -2k.$$

Also it can be shown, using a result by Frobenius [Fro96], that the multiplicity of each of these eigenvalues can be bounded in the following way:

$$m_p(\lambda_i) \leq \frac{p-1}{2},$$

for $0 \leq i < N$, where $m_p(\lambda)$ denotes the multiplicity of λ.
Now we need to link W_{2l} to the eigenvalues. The following equation can be easily shown by induction, as the left side is simply the trace of A^{2l}:

$$\sum_{j=0}^{N-1} \lambda_j^{2l} = NW_{2l}.$$

As all summands of the left hand side are positive we get:

$$\sum_{j=0}^{N-1} \lambda_j^{2l} > m_p(\lambda_1)\lambda_1^{2l}.$$

Now we apply the lower bound for the multiplicity and for $l > C(\epsilon)\log(p)$ we have:

$$\frac{p-1}{2}\lambda_1^{2l} < \sum_{j=0}^{N-1} \lambda_j^{2l} = NW_{2l} < |SL_2(\mathbb{F}_p)| \frac{(2k^{2l})}{p^{3-2\epsilon}}.$$

Now $|SL_2(\mathbb{F}_p)| = p(p^2-1) < p^3$ and thus we have:

$$\lambda_1^{2l} << \frac{(2k)^{2l}}{p^{1-2\epsilon}}.$$

For $l = C(\epsilon, \tau)\log(p)$ we get:

$$\lambda_1 < (2k)^{1-\frac{1-2\epsilon}{C(\epsilon)}} < 2k,$$

proving that:

$$\limsup_{n\to\infty} \lambda_1(A_{n,d}) < 2k = d,$$

and therefore that we have a family of expander graphs.

□

The only statement that remains to be shown to prove Theorem 2.21, is Lemma 2.23. To prove Lemma 2.23 we will need the following:

Lemma 2.24. *[BG08] Suppose $\nu \in \mathcal{P}(G)$ is a symmetric probability measure on G; that is,*

$$\nu(g) = \nu(g^{-1}),$$

satisfies the following three properties for fixed positive γ, $0 < \gamma < \frac{3}{4}$:

i)
$$\|\nu\|_\infty < p^{-\gamma},$$

ii)
$$\|\nu\|_2 > p^{-\frac{3}{2}+\gamma},$$

iii)
$$\nu^{(2)}[G_0] < p^{-\gamma}, \text{ for every proper subgroup } G_0.$$

Then for some $\epsilon(\gamma) > 0$, for all sufficiently large p:

$$\|\nu * \nu\|_2 < p^{-\epsilon} \|\nu\|_2$$

Lemma 2.24 is of the most interest to us, as its proof contains the aforementioned arguments from additive combinatorics.

Therefore, we will prove this statement in detail, and then pass quickly through the proof of Lemma 2.23 which is highly technical and not of interest in this context.

Proof of Lemma 2.24. We will prove this lemma by contradiction. Assuming that:

$$\|\nu * \nu\| \geq p^{-\epsilon} \|\nu\|_2 \tag{2.1}$$

and show that this assumption implies that there is a proper subgroup G_0 such that:

$$\nu^{(2)}[G_0] > p^{-\gamma}. \tag{2.2}$$

Our task is to construct a subgroup G_0 that leads to this desired contradiction to (iii). To do this we will apply methods from additive combinatorics and some of the results shown in Chapter 1.

The first result we need to use is the Balog-Szemerédi-Gowers Theorem (Theorem 1.30), so it is necessary to find a link between the probability measures from the lemma and the multiplicative energy $E(A, B)$ which is one of the prerequisites of the BSG-Theorem. This link is given by the following equation:

$$E(A, B) = \left|\{(a, a', b, b') \in A \times A \times B \times B : ab = a'b'\}\right| = \|\mathbb{1}_A * \mathbb{1}_B\|_2^2,$$

which can easily be deduced from the definition of $\|\mathbb{1}_A * \mathbb{1}_B\|_2$.

Set $J := 10 \log(p)$. Our next step is to define a new probability measure with the above equation in mind:

$$\tilde{\nu} := \sum_{j=1}^{J} 2^{-j} mathbbm 1_{A_j},$$

where A_j are the level sets of the measure ν:

$$A_j := \{x : 2^{-j} < \nu(x) \leq 2^{-j+1}\},$$

for $1 \leq j \leq J$.

After some easy computations we obtain:

$$\tilde{\nu}(x) \leq \nu(x) \leq 2\tilde{\nu}(x) + \frac{1}{p^{10}},$$

which in turn implies:

$$\|\tilde{\nu} * \tilde{\nu}\|_2 > p^{-\epsilon} \|\tilde{\nu}\|_2,$$

as 2.1 holds for ϵ arbitrarily small.

As $\tilde{\nu}$ was constructed with the definition of the multiplicative energy in mind, we are now able to find two sets A and B which fulfil the prerequisites of the BSG-Theorem.

We can find j_1 and j_2 such that:

$$p^{-2\epsilon}|A_{j_1}|^{\frac{3}{4}}|A_{j_2}|^{\frac{3}{4}} \leq \left\| \mathbb{1}_{A_{j_1}} * \mathbb{1}_{A_{j_2}} \right\|_2 = E(A_{j_1}, A_{j_2}),$$

and:

$$\min\left(2^{-j_1}|A_{j_1}|, 2^{-j_2}|A_{j_2}|\right) \geq \frac{p^{-\epsilon}}{J^2} \tag{2.3}$$

Let $A := A_{j_1}$ and $B := A_{j_2}$, then we have:

$$E(A, B) \geq p^{-4\epsilon}|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}.$$

Thus we can apply Corollary 1.32 which yields a set $A_1 \subset A$ such that:

$$|A_1| > p^{-\epsilon_1}|A| \text{ and } \left|A_1 A_1^{-1}\right| < p^{\epsilon_1}|A_1|,$$

where $\epsilon_1 := 4C_1\epsilon$ with an absolute constant C_1.

Using these properties we get the following bound for the Rusza distance between A_1 and A_1^{-1}:

$$d(A_1, A_1^{-1}) = \log\left(\frac{\left|A_1 A_1^{-1}\right|}{|A_1|}\right) < \epsilon_1 \log(p).$$

The set A_1 is the first step to constructing a proper subgroup which fulfils Equation 2.2. Using the bound for the Rusza distance, we will construct an approximate group H which in the end will be contained in our proper subgroup.

Theorem 1.28 can be used to make a connection between the Rusza distance and approximate groups.

Let $\epsilon_2 := C_2\epsilon_1$ with an absolute constant C_2. We apply Theorem 1.28 to obtain a p^{ϵ_2}-approximate group H with the following properties:

- $|H| < p^{\epsilon_2}|A_1|$,
- $A_1 \subset XH$ and
- $A_1 \subset HY$ with $|X||Y| < p^{\epsilon_2}$,

where Y and X are sets that result from the application of the theorem.

We need to find a $x_0 \in X$ such that $\nu(x_0 H)$ is as large as we need it to be. We can exploit the construction of $A = A_{j_1} \supset A_1$ to calculate $\nu(A) > 2^{-j_1}|A|$. Also there is a $x_0 \in X$ such that:

$$|A_1 \cap x_0 H| > p^{-\epsilon_2}|A_1|,$$

because $A_1 \subset \bigcup_{x \in X} xH$ and $|X| < p^{-\epsilon_2}$.
Combining this we get:

$$\nu(x_0 H) > \nu(A_1 \cap x_0 H) > 2^{-j_1} p^{-\epsilon_2} p^{-\epsilon_1} |A_{j_1}|.$$

Due to 2.3 we can reduce this inequality to:

$$\nu(x_0 H) > p^{-(\epsilon_1 + \epsilon_2 + 2\epsilon)} \tag{2.4}$$

As ϵ_1 and ϵ_2 depend on ϵ we can choose γ sufficiently small such that:

$$\nu(x_0 H) > p^{-\frac{\gamma}{2}}. \tag{2.5}$$

Because of the definition of $\nu^{(2)}$, this would yield the desired contradiction 2.2 if H were a proper subgroup. The final step of this proof will then be to find a subgroup G_0 which contains H, immediately contradicting (iii) and proving the result.
To find a proper subgroup we will use Lemma 1.33. If we can show that:

- $|H| < p^{3-\delta}$ for some $\delta > 0$ and
- $|H \cdot H \cdot H| < c|H|^{1+\kappa}$ with $c > 0$ and $\kappa > 0$ depending only on δ,

then Lemma 1.33 equips us with a proper subgroup G_0 of $SL_2(\mathbb{F}_p)$ containing H and we are done.
Due to the construction of the A_j we can rewrite 2.4 as:

$$|H| < p^{\epsilon_3} |A_1| \leq p^{\epsilon_3} |A_{j_1}| \leq p^{\epsilon_2} 2^{j_1}$$

After some more computations we can give a bound for 2^{j_1}:

$$2^{j_1} \leq p^{3 - 2\gamma + 4\epsilon}.$$

Combining these two inequalities yields:

$$|H| \leq p^{3 - 2\gamma + 4\epsilon + \epsilon_2},$$

which proves the first property.
To prove the second property we use this fact about approximate groups which was shown in Chapter 1:

$$|H \cdot H \cdot H| < p^{2\epsilon_2} |H|$$

Using (i) and 2.5 we get:

$$p^{-\epsilon_3} < \nu(x_0 H) \leq \sum_{x \in x_0 H} \nu(x) < |H| \, \|\nu\|_\infty < |H| p^{-\gamma}$$

Altogether we have:

$$|H \cdot H \cdot H| < |H|^{1+\frac{2\epsilon_2}{\gamma-\epsilon_3}},$$

as desired.

□

Using Lemma 2.24 we can prove Lemma 2.23:

Proof of Lemma 2.23. To prove this lemma we need to apply Lemma 2.24 to $\nu = \mu_{S_p}^{(l)}$ for $l \ \log(p)$ and a symmetric set of generators S_p of cardinality $2k$, such that the large girth condition of the lemma is fulfilled.

We will just assume that $\mu_{S_p}^{(l)}$ obeys all the conditions of Lemma 2.24, as proving this is highly technical and not of interest in this context.

Because $\mu^{(2l)}(1) = \left\|\mu_{S_p}^{(l)}\right\|_2^2$, as shown before, we can see that $\left\|\mu_{S_p}^{2l}\right\|_2 = \left\|\mu_{S_p}^{(l)}\right\|_2^2$ which implies:

$$\left\|\mu_{S_p}^{(l)}\right\| < p^{-\delta},$$

for some $\delta > 0$ depending only on γ from Lemma 2.24, which proves the statement.

□

This concludes the proof of Theorem 2.21. We still need to explain why Theorem 2.21 implies Theorem 2.20. Most of the work of this is done in the following lemma:

Lemma 2.25. *[Gam02] Let S be a symmetric set of elements in $SL_2(\mathbb{Z})$ such that $\langle S\rangle$ is a free group. Let $\alpha(S) := \max_{L\in S} \|L\|$. Then we we have:*

$$\operatorname{girth}(Cay(SL_2(\mathbb{F}_p), S_p)) \geq 2\log_\alpha\left(\frac{p}{2}\right)$$

As the proof of this lemma is mostly algebraic in nature, we will not state it here, but refer to [Gam02].

Now we have all the prerequisites for the proof of Theorem 2.20 and all that remains is to combine these:

Proof of Theorem 2.20. If $\langle S\rangle$ is a free group then Lemma 2.25 furnishes us with the lower bound of the girth that we need to apply Theorem 2.21. Thus the $Cay(SL_2(\mathbb{F}_p), S_p)$ form a family of expanders.

Otherwise we look at $\langle S\rangle \cap H$, where H denotes the Sanov group which is generated by the following elements:

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

It is a well known fact that H is a free group generated by these two elements [San47]. Therefore $\langle S\rangle \cap H$ is a free group and also a subgroup of $\langle S\rangle$, so that the large girth condition from Lemma 2.25 holds.

□

Theorem 2.20 completely resolves the question raised by Lubotzky, but Theorem 2.21 also has another interesting implication for random Cayley graphs, i.e. for Cayley graphs, whose set S is chosen independently at random:

Corollary 2.26. *[BG08] Fix $k \geq 2$. Let $g_1, \ldots, g_k$ be chosen independently at random in $SL_2(\mathbb{F}_p)$ and set $S_p^{rand} := \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$. There is a constant, $\kappa(k)$, independent of p such that as $p \to \infty$ asymptotically almost surely:*

$$\lambda_1(A(Cay(SL_2(\mathbb{F}_p), S_p^{rand}))) \leq \kappa < 2k$$

For the proof of this corollary we need the following lemma, whose proof however will not be presented here, as it deviates from our main interest:

Lemma 2.27. *[GHS09] Let d be a fixed integer greater than 2. As $p \to \infty$, asymptotically almost surely the girth of the d-regular random Cayley graph of $SL_2(\mathbb{F}_p)$ is at least:*

$$\left(\frac{1}{3} - o(1)\right) \cdot \log_{d-1}(|G|).$$

Proof of Corollary 2.26. As $Cay(SL_2(\mathbb{F}_p), S_p^{rand})$ is a $2k$-regular random Cayley graph Lemma 2.27 supplies us with a lower bound of the girth of this graph. This bound is enough to apply Theorem 2.21, which implies that the $Cay(SL_2(\mathbb{F}_p), S_p^{rand})$ are a family of expanders. The statement in the theorem follows from the algebraic characterisation of expanders.

□

As stated in the beginning of this section, the additive combinatorial approach to this type of problem was novel in [BG08].

This raises the question of whether similar techniques to the ones applied here might find use in the theory of expanders. Especially Lemma 2.24 seems very general and may even be applied outside the context of $SL_2(\mathbb{Z})$.

For this to be possible, however, it is necessary to find statements in the vein of Lemma 1.33 for other groups than $SL_2(\mathbb{Z})$. The theory of product estimates is still not as advanced as its commutative counterpart, but the statements found so far, indicate that, particularly for special groups, strong results are possible.

3 Addition Cayley Graphs and Additive Combinatorics

The former chapter has shown that additive combinatorics can be used to prove statements about Cayley graphs. However, it has not been possible to find any results on additive combinatorics using Cayley graphs in their proofs.

Even in the proof just shown for the expanding properties of Cayley graphs, it was necessary to use the non-commutative theory of additive combinatorics, which is in no way as advanced as the commutative theory.

Therefore, we will turn to a rather new variant of the Cayley graph: the addition Cayley graph. To differentiate more clearly between these two, we will sometimes refer to Cayley graphs as regular Cayley graphs.

By an addition Cayley graph we understand a particular variation on the Cayley graphs. In contrast to these, the addition Cayley graphs are only defined over abelian groups: The elements of an abelian group G form the vertex set, and two vertices are connected by an edge, if their sum is in a given set $S \subseteq G$.

While regular Cayley graphs are widely studied and there is a great expanse of literature concerning these, addition Cayley graphs have been largely disregarded or overlooked. In fact it is possible to give a nearly conclusive list of all the literature on addition Cayley graphs [GLS07]:

- One of the earliest papers by Chung concerns expander properties and the diameter [Chu89];
- On the Hamiltonicity [CGW03];
- On the clique number [Gre05];
- On the independence number [Alo07].

To the papers above mentioned in [GLS07] we can add:

- On connectivity [GLS07];
- More on Hamiltonicity [Lev10];
- and a conjecture on the Hamiltonicity [CL]
- A paper on $(3, 6)$-fullerenes [DGMS09];
- in this paper [AABL09] addition Cayley graphs are used to prove a result on expanders;

Addition Cayley graphs are known in the literature under several different names:

- sum graphs [Gre05];
- addition graphs [CGW03];
- Cayley sum graphs [Alo07];
- addition Cayley graphs [GLS07], [Lev10].

Here we will adopt the name of addition Cayley graph, as [GLS07] gives the most conclusive definition. This way we can also avoid confusion with the related (integral) sum graphs and mark the relation to regular Cayley graphs.

In section 3.1 we will formally introduce addition Cayley graphs and show some basic properties.

In section 3.2 and 3.3 we will present results by B. Green [Gre05] and N. Alon [Alo07], respectively. The aim of these two sections is to show that there is a two-way relationship between the theories of additive combinatorics and addition Cayley graphs, hopefully establishing addition Cayley graphs as a useful tool to transfer results from graph theory to additive combinatorics and vice versa.

While [Gre05] uses methods of additive combinatorics to gain information on the clique number of addition Cayley graphs, [Alo07] exploits results from graph theory to estimate the number of independent sets in addition Cayley graphs, which he in turn uses to give an upper bound to the size of sumsets in $\mathbb{Z}_p$.

3.1 Addition Cayley Graphs

Definition 3.1. (addition Cayley graph) Let G be a finite abelian group and $S \subseteq G$ a subset of G. We define the *addition Cayley graph* induced by S on G, $Cay_G^+(S)$, to be the undirected graph with the vertex set G and the edge set $E(Cay_G^+(S)) := \{\{g_1, g_2\} \in G \times G : g_1 + g_2 \in S\}$.

In the special case that the set $S \subseteq G$ is square free, i.e. contains no elements of the form $g = h + h$ with $h \in G$, the graph $Cay_G^+(S)$ is regular of degree $|S|$. In general every vertex $g \in G$ has either degree $|S| - 1$ if and only if $g + g \in S$ or degree $|S|$ otherwise (that is if we do not count loops). Figures 3.1 and 3.2 are examples for $\mathbb{Z}_9$ and $\mathbb{Z}_{10}$ respectively.

Remark 3.2. The definition of addition Cayley graphs already reveals a close resemblance to the standard Cayley graphs. But there also some differences between these two objects:

- If G is an abelian group we can define the edge set of standard Cayley graphs as $E\left(Cay(G, S)\right) := \{\{v, w\} : v - w \in S\}$, which definition is well founded as the set S is symmetric.

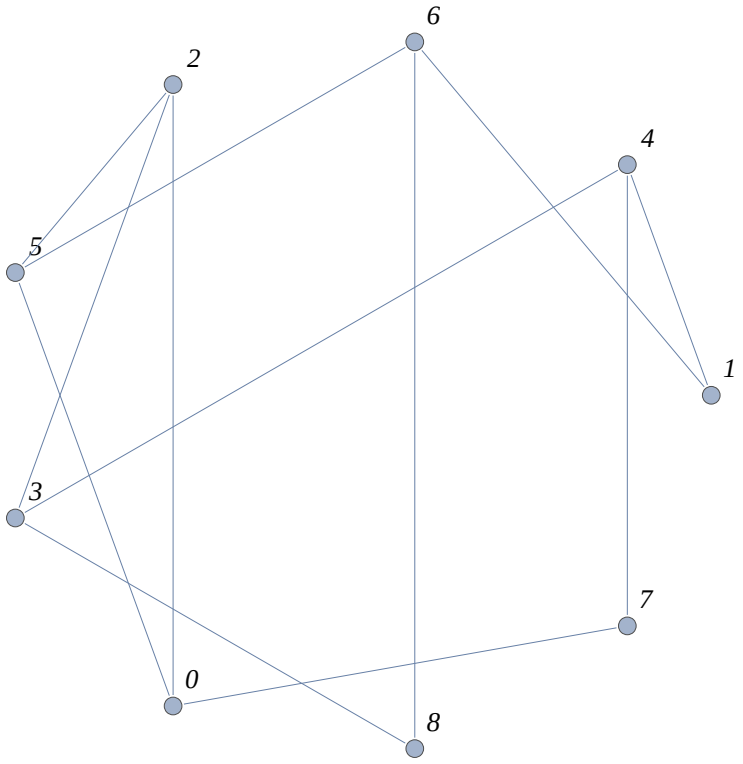


Figure 3.1: $Cay^+_{\mathbb{Z}_9}(\{2,5,7\})$ without self-loops

- The square of an addition Cayley graph $Cay^+_G(S)$ is in fact the standard Cayley graph $Cay(G, S - S\backslash\{0\})$.
- In contrast to standard Cayley graphs, addition Cayley graphs are not vertex transitive.

The following theorem shows for which subsets $S \subseteq G$ the graph $Cay^+_G(S)$ is connected:

Theorem 3.3. *[Lev10] Let G be a finite abelian group and let $S \subseteq G$. $Cay^+_G(S)$ is connected if and only if one of the following statements is true:*

i) S is not contained in a coset of a proper subgroup of G.

ii) S is contained in the non-zero coset of an index 2 subgroup of G, but not contained in any other coset.

Proof. The cases where G is trivial and where S is empty are easy to check. Assume that G is non-trivial and that S is not empty. Let H be the smallest subgroup of G such that S is contained in a coset of H, i.e. H is the subgroup generated by the difference set $S - S$. The connected component of $Cay^+_G(S)$ containing 0 consists of all those elements

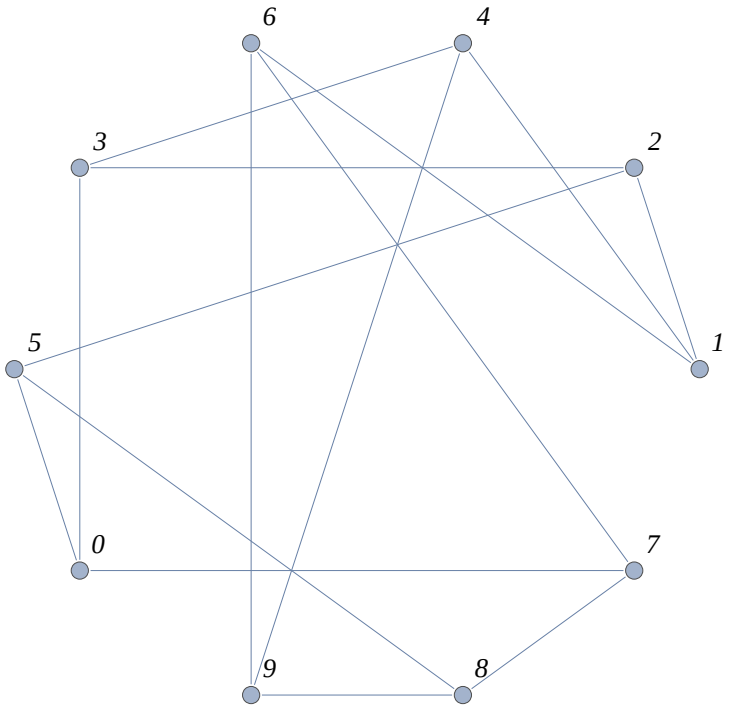


Figure 3.2: $Cay^+_{\mathbb{Z}_{10}}(\{3,5,7\})$ without self-loops

of G representable as $s_1 - s_2 + s_3 - \ldots + (-1)^{k+1}s_k$ with $k \geq 0$ and $s_1, \ldots, s_k \in S$. Therefore this component is the set $H \cup (S + H)$. Thus $Cay^+_G(S)$ is connected if and only if either $H = G$ or H is a subgroup of index 2, implying that $S \subseteq G \backslash H$.

□

The following is a generalisation of a result in [CGW03]:

Proposition 3.4. *Let G be a group and S be contained in the non-zero coset of an index 2 subgroup of G, but not in any other coset. Then the graph $Cay^+_G(S)$ is bipartite.*

Proof. Let S be contained in the non-zero coset of the index 2 subgroup of H. Then $H = \langle S - S \rangle$ and $G = H \cup H + s$, where $s \in S$.

Let $e = \{g_1, g_2\}$, $g_1, g_2 \in G$, $e \in E\left(Cay^+_G(S)\right)$:

Suppose $g_1 \in H$. As $e \in E\left(Cay^+_G(S)\right)$, $g_2 = s^* - g_1$ for an $s^* \in S$. Therefore $g_2 \in H + s$.

Suppose $g_1 \in H + s$. Again $g_2 = s^* - g_1$ for an $s^* \in S$. As $g_1 \in H + s$, we see that $g_1 = h + s$ for some $h \in H$. Therefore $g_2 = (s * -s) - h$ and $g_2 \in H$.

Thus $Cay^+_G(S)$ is bipartite with partition $V\left(Cay^+_G(S)\right) = H \cup H + s$.

□

As with regular Cayley graphs, it is possible to compute the eigenvalues of $Cay^+_G(S)$ using characters:

Theorem 3.5. *[DGMS09] Let G be a finite abelian group and $S \subseteq G$. The multiset of eigenvalues of $Cay^+_G(S)$ is:*

$$\left\{\sum_{s\in S}\chi(s) : \chi \in R\right\} \cup \left\{\pm|\sum_{s\in S}\chi(s)| : \chi \in C\right\},$$

where $R := \{\chi_a : a + a = 0\}$ is the set of real valued characters of $Cay^+_G(S)$ and C is the set containing exactly one character from $\{\chi_a, \chi_{-a}\}$ for each $a \in G$ with $a + a \neq 0$.

Proof. Let χ be a character of G and $u \in G$ a vertex of $Cay^+_G(S)$. Then:

$$\sum_{v\in N(u)}\chi(v) = \sum_{s\in S}\chi(s-u) = \left(\sum_{s\in S}\chi(s)\right)\cdot\overline{\chi(u)}$$

Therefore every real valued character is an eigenvalue corresponding to the eigenvalue $\sum_{s\in S}\chi(s)$.

If $\chi \in C$, then it is not an eigenvector. Choose $\alpha \in \mathbb{C}$, such that $|\alpha| = 1$ and $\alpha^2\sum_{s\in S}\chi(s) = \left|\sum_{s\in S}\chi(s)\right|$. Let $u \in G$:

$$\sum_{v\in N(u)}\alpha\chi(v) = \left(\alpha^2\sum_{s\in S}\chi(s)\right)\cdot\alpha^{-1}\overline{\chi(u)} = \left|\sum_{s\in S}\chi(s)\right|\cdot\overline{\alpha\chi(s)}$$

Therefore $Re(\alpha\chi)$ and $Im(\alpha\chi)$ are real eigenvectors to eigenvalues $\left|\sum_{s\in S}\chi(s)\right|$ and $-\left|\sum_{s\in S}\chi(s)\right|$, respectively.

□

3.2 The Clique Number and Small Sumsets

Having introduced the addition Cayley graphs in the former section, we would like to show that there is a strong tie between these graphs and the field of additive combinatorics.

Therefore, in this section we will present a result by B. Green [Gre05], which gives an estimate for the clique number of a random addition Cayley graph using additive combinatorics.

The result is the following:

Theorem 3.6. *[Gre05] Let $S \subseteq \mathbb{Z}_N$ be chosen randomly from $\mathbb{Z}_N$. Let ω denote the clique number of $Cay^+_{\mathbb{Z}_N}(S)$. Then we have:*

$$\lim_{N\to\infty}\mathbb{P}\left(\omega \leq 160\log(N)\right).$$

If we are able to prove this, we get the following result in Ramsey theory as a corollary:

Corollary 3.7. *[Gre05] For all sufficiently large integers N there exists a set $S \subseteq \mathbb{Z}_N$ for which the addition Cayley graph $Cay^+_{\mathbb{Z}_N}(S)$ has no cliques or independent sets of size $160\log(N)$.*

A clique in graph theoretical terms is just a subset of $V(\mathcal{G})$, say X, such that for each $v, w \in X$ we have $\{v, w\} \in E(\mathcal{G})$.

To use additive combinatorics to find the clique number of an addition Cayley graph, we need a characterisation of a clique using terms from this field.

A clique of an addition Cayley graph $Cay^+_G(S)$ is a set $X \subseteq G$ such that for each $g_1, g_2 \in X$ with $g_1 \neq g_2$ we have $g_1 + g_2 \in S$. This characterisation relates to a notion named the restricted sumset:

Definition 3.8. (restricted sumset) Let A be an additive set in an ambient group Z. Then:

$$|A\hat{+}A| := \{a_1 + a_2 : a_1, a_2 \in A; a_1 \neq a_2\}$$

Using this, it is easy to see that the following two statements are equivalent:

i) X is a clique of $Cay^+_G(S)$

ii) $X\hat{+}X \subseteq S$.

To prove Theorem 3.6 we need to estimate the number of such sets, i.e. the number of cliques in the graph.

Notation 3.9. By $S^m_k(G)$ we will denote the collection of sets X with $|X| = k$ and $|X\hat{+}X| = m$. We will call $|X\hat{+}X| = m$ the *small doubling property.*

Using this notation we can calculate the expected number of k-cliques in a random addition Cayley graph $Cay^+_G(S)$, which we denote by $\mathbb{E}(G, k)$:

$$\begin{aligned}
\mathbb{E}(G,k) &= \sum_{X\subseteq G:|X|=k} \mathbb{P}(X \text{ is a clique in } Cay^+_G(S)) \\
&= \sum_{m\geq k-1} \sum_{X\in S^m_k(G)} \mathbb{P}(X\hat{+}X \subseteq S) \\
&= \sum_{m\geq k-1} \sum_{X\in S^m_k(G)} 2^{-m} \\
&= \sum_{m\geq k-1} |S^m_k(G)|\, 2^{-m},
\end{aligned} \tag{3.1}$$

as $S^m_k(G)$ is empty for $m < k - 1$.

Thus we only need to bound the last element of this equation, i.e. bound S^m_k. Because the doubling constant (or in our case $|X\hat{+}X|$) is invariant under 2-Freiman isomorphisms, it will be enough to estimate the number of subsets of G that are 2-isomorphic to X,

with $X \subset G$, $|X| = k$ and $|X\hat{+}X| = m$ (i.e. the size of an isomorphism class with the small doubling property) and then multiply this value with the number of isomorphism classes.

As we are interested in addition Cayley graphs over the group $\mathbb{Z}_N$, we can lift $X \subset \mathbb{Z}_N$ to the integers using an unfolding map. This enables us to estimate the sets 2-isomorphic to the lift of X, which in practice is more efficient.

The first step, estimating the size of the isomorphism classes has already been shown in Theorem 1.48. Therefore, we only need to estimate the number of isomorphism classes, as explained above.

This will be done in Lemma 3.12. The following Lemmas 3.10 and 3.11 are just necessary prerequisites.

Lemma 3.10. *[Gre05] Suppose that $A \subseteq W$ has sufficiently large cardinality $k = |A|$ and let $m = |A\hat{+}A|$. Then there exists $a^* \in A$ and $A_0, A_1 \subseteq A$ such that:*

- $|A_0| \leq 4k^{-\frac{1}{15}}m$
- $|A \backslash A_1| \leq 4k^{-\frac{4}{5}}m$
- $a^* + A_1 \subseteq A_0\hat{+}A_0$

Proof. Let $C := \left\lfloor k^{\frac{1}{5}} \right\rfloor$ and $c := k^{-\frac{1}{15}}$. We construct a graph $\mathcal{G}$ the following way: Let $V(\mathcal{G}) := A$ and let there be an edge between to vertexes $x, y \in A$, if the number of pairs $(w, z) \in A \times A$ with $w + z = x + y$ and $w \neq z$ is less than C.

As there are no more than Cm edges in $\mathcal{G}$, there is a vertex a^* which has degree at most $\frac{2Cm}{k}$. Pick a set $X \subseteq A$ by choosing independently and at random each $a \in A$ to be in X with probability c.

Let Z:= $\{a \in A : a^* + a \notin X\hat{+}X\}$. If $\{a, a^*\} \notin E(\mathcal{G})$ then there are at least $\frac{C}{3}$ disjoint pairs $(a_1, a_2) \in A \times A$ with $a_1 + a_2 = a^* + a$ and $a_1 \neq a_2$. The probability that both a_1 and a_2 are in X is c^2 and thus:

$$\mathbb{P}(a \in Z) \leq \left(1 - c^2\right)^{\frac{C}{3}} \leq e^{-c\frac{C}{3}}.$$

Therefore we get:

$$\mathbb{E}|Z| \leq \frac{2Cm}{k} + e^{-q^2\frac{C}{3}}k \leq 3k^{-\frac{4}{5}}m,$$

and with $\mathbb{E}|X| = ck = k^{14}15$:

$$\mathbb{E}\left(|X| + k^{\frac{14}{15}}|Z|\right) \leq 4k^{-\frac{1}{15}}m.$$

Now we can pick a set $X \subseteq A$ such that $|X| + k^{\frac{14}{15}}|Z| \leq 4k^{-\frac{1}{15}}m$. The result follows by setting $A_0 = X$ and $A_1 = A\backslash Z$.

□

Lemma 3.11. *[Gre05] Fix a non-negative integer t and a set $B \subset W$ of cardinality $|B| = l$. Then the number of mutually non-isomorphic sets A of cardinality $|A| = l + t$, such that there exists a subset $A_0 \subseteq A$ satisfying $A_0 \cong_3 B$, is at most l^{3t^4}.*

Proof. Suppose we have A of cardinality $l+t$ such that there exists subset $A_0 \subset A$ with $A \cong_3 B$. Denote $B := \{b_1, \ldots, b_l\}$, $A_0 := \{a_1, \ldots, a_l\}$ and $A := A_0 \cup \{a_{l+1}, \ldots, a_{l+t}\}$, such that for all $i_1, \ldots, i_6 \in \{1, \ldots, l\}$:

$$b_{i_1} + b_{i_2} + b_{i_3} = b_{i_4} + b_{i_5} + b_{i_6}$$

if and only if

$$a_{i_1} + a_{i_2} + a_{i_3} = a_{i_4} + a_{i_5} + a_{i_6},$$

which is possible as $A_0 \cong_3 B$.

□

Now we have the necessary information to give an estimate on the size of an isomorphism class with the small doubling property:

Lemma 3.12. *[Gre05] Let k be a sufficiently large positive integer and let $m \leq k^{\frac{31}{30}}$. Then the number of isomorphism classes of $A \subseteq F^k$ with $|A| = k$ and $|A\hat{+}A| \leq m$ is at most $\left(\frac{em}{k}\right)^k e^{k^{31/32}}$.*

Proof. Let $A \subseteq F^k$ with $|A| = k$ and $|A\hat{+}A| \leq m$: Then by Lemma 3.10 there exists an $a^* \in A$ and $A_0, A_1 \subseteq A$ such that:

- $|A_0| \leq 4k^{-\frac{1}{15}}m$,
- $|A_1| \geq |A| - 4k^{-\frac{4}{5}}m$, and
- $a^* + A_1 \subseteq A_0\hat{+}A_0$.

The number M of possible Freiman 6-isomorphism classes to which A_0 can belong can be determined with Lemma 1.41. After some computations we get $M < e^{k^{30/31}}$ and we can pick representatives of these classes $X_1, \ldots, X_M$.

We know that $A_0\hat{+}A_0$ is Freiman 3-isomorphic to $X_i\hat{+}X_i$ for all $1 \leq i \leq M$ (Lemma 1.40). Also, as $a^* + A_1 \subseteq A_0$, there is a non-empty subset of some $X_i\hat{+}X_i$ which is Freiman 3-isomorphic to $a^* + A_1$.

The number of Freiman 3-isomorphism classes in $X_i\hat{+}X_i$ will certainly be less than the number of subsets of cardinality k which is $\binom{m}{k} \leq \left(\frac{em}{k}\right)^k$. As $|A_1| \leq k$ it can belong to at most $Mk\left(\frac{em}{k}\right)^k$.

We use Lemma 3.11 to see that for each of the 3-isomorphism classes and for any $t \leq 4k^{-\frac{4}{5}}m$ there are at most $e^{k^{31/32}}$ isomorphism classes for A. Thus we have the following number of isomorphisms altogether:

$$e^{k^{30/31}} \cdot k\left(\frac{em}{k}\right)^k \cdot 4k^{-\frac{4}{5}} \cdot e^{k^{29/30}} < \left(\frac{em}{k}\right)^k e^{k^{31/32}}$$

□

This result, however, is not very useful if the doubling constant is very small, in our case $m \leq 7k$. Lemma 3.13 and Corollary 3.14 will show us, that we do not need to consider sets with such small doubling.

Lemma 3.13. *[Gre05] Let k be a sufficiently large positive integer and let A be a subset of an abelian group with $|A| = k$. Let $\epsilon > 0$ be sufficiently small. Then there is a set $B \subseteq A$ with:*

$$|B| \leq \frac{3\log\left(\frac{1}{\epsilon}\right)}{\epsilon}\sqrt{k}$$

and $|B\hat{+}B| \geq (1-\epsilon)k$.

Proof. Let $p = 3\epsilon^{-1}\sqrt{\frac{\log(\frac{6}{\epsilon})}{2k}}$. Choose a set $B \subseteq A$ by picking each element of k independently at random with probability p. Using arguments from the probabilistic method, which we will not state here (see [Gre05]), we get the following estimate:

$$\mathbb{P}\left(||B| - pk| \geq \frac{\epsilon pk}{3}\right) < 2e^{-\frac{2\epsilon^2 p^2 k}{9}} = \frac{\epsilon}{3}. \tag{3.2}$$

For $x \in B\hat{+}B$ we define $s(x)$ to be the number of ordered pairs $(b_1, b_2) \in B^2$ with $b_1 \neq b_2$ and $b_1 + b_2 = x$. It is easy to see that the sum $\sum_{x\in B\hat{+}B} s(x)^2$ equals the cardinality of the set $\hat{E}(B)$ (a sort of restricted additive energy) of quadruples $(b_1, b_2, b_3, b_4) \in B^4$ with $b_1 + b_2 = b_3 + b_4$ and $b_1 \neq b_2$, $b_3 \neq b_4$.

We now need to calculate the expected size of $\hat{E}(B)$. For this we turn our attention to $\hat{E}(A)$. We can split this set into two disjoint sets $\hat{E}(A) = E_1 \cup E_2$ where:

$$E_1 := \{(a_1, a_2, a_3, a_4) \in A^4 : a_1 \neq a_2 \neq a_3 \neq a_4\}$$

and

$$E_2 := \{(a_1, a_2, a_3, a_4) \in A^4 : a_1 = a_3, a_2 = a_4 \vee a_1 = a_4, a_2 = a_3\}.$$

Obviously we have $|E_1| \leq k^3$ and $|E_2| \leq 2k^2$. The probability that an element x is contained in $E_1 \cap B^4$ is less than k^3p^4, while the probability that x is in $E_2 \cap B^4$ is $2k^2p^2$.

Thus the expected size of our set is:

$$\mathbb{E}\left(\sum_{x\in B\hat{+}B} s(x)^2\right) = \mathbb{E}(|\hat{E}(B)|) = \mathbb{E}(|E_1 \cup E_2|) \leq 2k^2p^2 + k^3p^4.$$

From this inequality we get:

$$\mathbb{P}\left(\sum_{x\in B\hat{+}B} s(x)^2 \leq \frac{2k^2p^2 + k^3p^4}{1 - \frac{\epsilon}{3}}\right) \geq \frac{\epsilon}{3}. \tag{3.3}$$

Because of 3.2 and 3.3 we can pick a set B with the following properties:

$$||B| - pk| \leq \frac{\epsilon pk}{3} \text{ and } \sum_{x \in B \hat{+} B} s(x)^2 \leq \frac{2k^2p^2 + k^3p^4}{1 - \frac{\epsilon}{3}}.$$

With Cauchy-Schwarz we get:

$$\sum_{x \in B \hat{+} B} s(x)^2 \geq \frac{|B|^2 \left(|B| - 1\right)^2}{|B \hat{+} B|},$$

which leads to:

$$|B \hat{+} B| \geq (1 - \epsilon)k.$$

By combining all of these inequalities and after some computation we get:

$$|B| \leq pk(1 + \frac{\epsilon}{3}) \leq \frac{3 \log\left(\frac{1}{\epsilon}\right)}{\epsilon} \sqrt{k}$$

□

Corollary 3.14. *[Gre05] Let k be a sufficiently large positive integer and let A be a subset of an abelian group with $|A| = k$. Then A contains a subset C, with:*

- $|C| \geq \frac{k}{8}$ *and*
- $|C \hat{+} C| \geq 7|C|$.

Proof. Apply Lemma 3.13 with $\epsilon = \frac{1}{9}$. We get a set B with $|B| \leq 100\sqrt{k}$, such that $|B \hat{+} B| \geq \frac{8k}{9}$. We get C by adding elements of A to B until $\frac{k}{8} \leq |C| \leq \frac{8k}{63}$.

□

We now have efficient estimates for both number and size of isomorphism classes, which have the small doubling property. Lemma 3.16 will show us how to deal with the aforementioned lift to the integers. It is a direct result of this classic result by Freiman:

Proposition 3.15. *[Fre73] Let $A \subseteq \mathbb{Z}$ have cardinality k and Freiman dimension $r_{\mathbb{Q}}(A)$. Then we have the inequality:*

$$|A \hat{+} A| \geq r \left(k - \frac{r+1}{2}\right).$$

The proof of this proposition is only a simple induction, but as it uses convex polyhedra, which we do not wish to introduce here, we refer to [Fre73].

Lemma 3.16. *[Gre05] Suppose that $A \subseteq \mathbb{Z}_N$ has cardinality k and that $|A \hat{+} A| = m$. Let $\overline{A}$ be the image of A under the unfolding map $\mathbb{Z}_N \hookrightarrow \mathbb{Z}$. Then we have:*

$$r_{\mathbb{Q}}(\overline{A}) \leq \frac{4m}{k}.$$

Proof. We get $r_{\mathbb{Q}}(\overline{A}) \leq k-1$, as $\overline{A}$ is a set of k integers. Applying Proposition 3.15, we have:

$$2m \geq |\overline{A}\hat{+}\overline{A}| \geq r_{\mathbb{Q}}(\overline{A})\left(k - \frac{r+1}{2}\right) \geq \frac{1}{2}kr_{\mathbb{Q}}(\overline{A}).$$

□

We will first bound $|S_k^m(\mathbb{Z}_N)|$ and then go on to bound the whole sum of Equation 3.1 in the proof of Theorem 3.6.

Lemma 3.17. *[Gre05] We have the bounds:*

$$|S_k^m(\mathbb{Z}_N)| \leq N^{1+\frac{4m}{k}}\left(\frac{2em}{k}\right)^k e^{k^{\frac{31}{32}}}$$

if $m \leq \frac{k^{\frac{31}{30}}}{2}$ *and*

$$|S_k^m(\mathbb{Z}_N)| \leq N^{1+\frac{4m}{k}}k^{4k}$$

whatever the value of m*.*

Proof. To prove this lemma we need to find bounds for the number of sets $A \in S_k^m(\mathbb{Z}_N)$. By the definition of S_k^m we have $|A| = k$ and $|A\hat{+}A| = m$. It will prove to be easier to count not the sets A directly, but their image $\bar{A}$ under the unfolding map $\mathbb{Z}_N \hookrightarrow \mathbb{Z}$. We pick $X_1, \ldots, X_M$ to be a complete set of representatives of the Freiman 2-isomorphism classes of subsets $X \subseteq \mathbb{Z}$ with $|X| = k$ and $|X\hat{+}X| \leq 2m$. We get:

$$M \leq k^{4k}$$

by Lemma 1.41. When $m \leq k^{\frac{31}{32}}$ we get:

$$M \leq \left(\frac{2em}{k}\right)^k e^{k^{31/32}}.$$

As $X_1, \ldots, X_M$ is a complete set of representatives every $\bar{A}$ is the image of some X_i under a Freiman 2-isomorphism $\psi : X_i \to \{1, \ldots, N\}$. By Theorem 1.48(i) there are at most $N^{r_{\mathbb{Q}}(X_i)+1}$ such isomorphisms.

By applying Lemma 3.16 we get the necessary inequalities.

□

Now we have all the information we need to prove Theorem 3.6:

Proof of Theorem 3.6. Let $k = \lfloor 20\log(N)\rfloor$. As mentioned in the beginning of this section we need to give an upper bound for:

$$\sum_{m \geq 7k} |S_k^m(\mathbb{Z}_N)|\, 2^{-m}.$$

To be able to use the bounds from Lemma 3.17, we need to split this sum into two parts according to whether $m \leq k^{\frac{31}{32}}$ or not. With some computations we get this upper bound:

$$\sum_{m=7k}^{\left\lfloor \frac{k^{31/32}}{2} \right\rfloor} 2^{m\left(\left(\frac{4}{k}+\frac{1}{m}\right)\log(N)+\frac{k}{m}\log(\frac{2em}{k})-1+o(1)\right)} + \sum_{m\geq\left\lfloor \frac{k^{31/32}}{2} \right\rfloor} 2^{m\left(\frac{4\log(N)}{k}-1+o(1)\right)}.$$

As $\frac{\log(2eC)}{C-1} \leq -0.2499$ when $C \geq 7$ (where C loosely represents $\frac{m}{k}$), both of these last sums, in that case, are bounded from above by N^{-2} for N sufficiently large.

Let S be a random subset of $\mathbb{Z}_N$. If there is a X with cardinality k for which $X\hat{+}X \subseteq S$, then by Lemma 3.14 there exists a set Y with:

- $Y\hat{+}Y \subseteq S$,
- $|Y| \geq \frac{k}{8}$ and
- $|Y\hat{+}Y| \geq 7|Y|$.

But in such a case the expected number of sets Y that are contained in S is bounded by N^{-2}, as $\frac{m}{k} \geq 7$. Therefore, A almost surely does not contain any $X\hat{+}X$ with $|X| = \lceil 160\log(N)\rceil$, proving the theorem.

□

In [Gre05] B. Green remarks that the the number 160 in the statement of Theorem 3.6 could be reduced to as far as $(3+\epsilon)$ using more refined methods than in this proof.

It would be interesting to discuss this question for other groups than the ones presented here (i.e. $\mathbb{Z}_N$) and in [Gre05] (i.e. $\mathbb{Z}_2^n$), although this appears to be very difficult.

In [Gre05] B. Green only deals with random Cayley graphs. Using the observation that cliques are equivalent to particular restricted sumsets, it is also possible to make statements on non-random addition Cayley graphs using results on the restricted sumset; for instance in [NA95] and [NA96] it is shown that:

$$|A+B| \geq \min\{p, |A|+|B|-2-\delta\}.$$

Also in [Lev05] V.F. Lev conjectures that:

Conjecture 3.18. *[Lev05] Let G be an abelian group and let A and B be finite non-empty subsets of G and let $\nu_{A,B}(c)$ denote:*

$$\nu_{A,B}(c) = |\{(a,b) \in A \times B : a+b=c\}|.$$

Then we have:

$$|A\hat{+}B| \geq |A|+|B|-2-\min_{c\in A+B}\nu_{A,B}(c).$$

Either of these two statements can be used to gain more information on the clique number of addition Cayley graphs.

3.3 The Independence Number and Large Sumsets

In this section we will prove a result about sumsets by means of addition Cayley graphs. Before we can state this result, however, we need to introduce some notation:

Notation 3.19. From now on in this chapter we will call a subset S of $\mathbb{Z}_p$, with $p > 2$ prime, a *sumset*, if there is a set $A \subset \mathbb{Z}_p$ such that $A + A = S$.

With $f(p)$ we shall denote the maximum integer f such that every $S \subset \mathbb{Z}_p$ of size at least $p - f$ is a sumset.

It will be our aim to bound $f(p)$ from above as follows:

Theorem 3.20. *[Alo07] For all sufficiently large p there exists an $F \subset \mathbb{Z}_p$ of cardinality $16\frac{p^{\frac{2}{3}}}{\log^{\frac{1}{3}} p}$ so that $S = \mathbb{Z}_p - F$ is not a sumset. Thus there exists a positive constant c and an integer p_0 so that for all $p > p_0$:*

$$f(p) < c\frac{p^{\frac{2}{3}}}{\log^{\frac{1}{3}} p}.$$

In [Alo07] N. Alon also establishes a lower bound for $f(p)$. But we are only interested in the application of addition Cayley graphs, and will thus concentrate on the upper bound.

To prove this upper bound we need to find a set $F \subset \mathbb{Z}_p$ of size $|F| \leq \mathcal{O}\left(\frac{p^{\frac{2}{3}}}{\log^{\frac{1}{3}}(p)}\right)$ such that $T := \mathbb{Z}_p - F$ is not a sumset. We will view T as the disjoint union of sets S and S' each of size $\mathcal{O}\left(\frac{p^{\frac{2}{3}}}{\log^{\frac{1}{3}}(p)}\right)$.

We will choose the set S first. For any S' suppose that $T = \mathbb{Z}_p - (S \cup S')$ is a sumset, say $A + A$. Obviously $A + A$ and S must be disjoint. Now all we have to do is compare the number of sets $A \subseteq \mathbb{Z}_p$ whose square is disjoint with S to the number of possibilities for S'. If we can show that there are less options for a set A, than for S', then there has to be a set S' such that $\mathbb{Z}_p - F = \mathbb{Z}_p - (S \cup S')$ is not a sumset, which is what we want to prove. So to prove the result we will need to find an upper bound for the number of sets A with $(A + A) \cap S = \emptyset$.

To do this we will use addition Cayley graphs. It is easy to see that our property $(A + A) \cap S = \emptyset$ is equivalent to A being an independent set in $Cay^{+}_{G}(S)$. So finding the needed upper bound will be equivalent to finding an upper bound of independent sets in addition Cayley graphs.

Addition Cayley graphs for which loops have been allowed are a special case of (n, d, λ)-graphs.

As (n, d, λ)-graphs are an important part of the theory of expanders, there are many results about their properties and in particular one about the number of independent sets:

Lemma 3.21. *[AR05] Let G be a (n, d, λ)-graph, and suppose $m \geq \frac{2n\log(n)}{d}$. Then the number of independent sets of size m in G is at most:*

$$\left(\frac{emd^2}{4\lambda n \log(n)}\right)^{\frac{2n\log(n)}{d}} \left(\frac{2e\lambda p}{md}\right)^m$$

To prove this result we will need the following lemma:

Lemma 3.22. *[AR05] Let $\mathcal{G}$ be a (n, d, λ)-graph, and let $B \subset V(\mathcal{G})$ be a subset of bn vertices of $\mathcal{G}$. Define:*

$$C = \{u \in V(\mathcal{G}) : |N(u) \cap B| \leq \frac{db}{2}\},$$

where $N(u)$ includes u itself, if there is a loop at u. Then:

$$|B||C| < \frac{4\lambda^2}{d^2} n^2.$$

In particular, if $|B| \geq \frac{2\lambda}{d} n$ then $|C| < \frac{2\lambda}{t} n$, and consequently for every $B \subset V(\mathcal{G})$, $|B \cap C| < \frac{2\lambda}{d} n$.

Proof. Let $A := A(\mathcal{G})$ and define a vector $x = (x_v : v \in V(\mathcal{G}))$ by $x_v = -b$ if $v \notin B$ and $x_v = 1 - b$ if $v \in B$. We get:

$$\|Ax\|_2^2 = x^t A^t A x \leq \lambda^2 x^t x.$$

We can compute the value of $xx^t = (n - |B|)b^2 + |B|(1-b)^2 = b(1-b)n$ and therefore we have:

$$\|Ax\|_2^2 = \sum_{v \in V} (|N(v) \cap B|(1-b) - (d - |N(v) \cap B|)b)^2 = \sum_{v \in V} (|N(v) \cap B| - db)^2$$

Combining all this results in:

$$\sum_{v \in V} (|N(v) \cap B| - db)^2 \leq \lambda^2 x^t x = \lambda^2 b(1-b)n.$$

Because of the choice of C we can infer that:

$$|C| \frac{d^2 b^2}{4} < \lambda^2 b(1-b)n < \lambda^2 bn,$$

slightly modifying this inequality leads to the desired result.

□

Now we are able to prove the statement about independent sets in (n, d, λ)-graphs:

Proof of Lemma 3.21. In the following we will choose an ordered set $v_1, \ldots, v_m$ of m vertices that form an independent set for $\mathcal{G}$. The vertex v_{i+1} will always be chosen from the set B_i, which is still to be defined. To prove the result we need to find out how many ways there are to choose such a set.

We define sets B_i inductively in the following way: Let $B_0 := V(\mathcal{G})$. We then let B_i denote the set of all vertices that are not adjacent to the first i chosen vertices $v_1, \ldots, v_i$. Obviously we have $B_j \subset B_i$ for all $j > i$.

Next we define the following sets:

$$C_i := \{u \in V : |N(u \cap B_i)| \leq \frac{d|B_i|}{2n}\}.$$

Suppose we have vertices $v_1, \ldots, v_i$ as described above. Then, if the vertex we choose next, v_{i+1}, is not a member of C_i, we have: $|B_{i+1}| < \left(1 - \frac{d}{2n}\right)|B_i|$. If we choose more than $r := \frac{2n}{d}\log(n)$ vertices of this type our corresponding B_i (the set of all non-neighbours) will be empty, making it impossible to choose another vertex for our ordered set.

Thus with at most r possible exceptions, each vertex v_{i+1} must lie in $B_i \cap C_i$ and by Lemma 1.41 the set $B_i \cap C_i$ is of size at most $\frac{2\lambda}{d}n$.

The number of possibilities to choose the indices of vertices that are not in $B_i \cap C_i$ can be bounded by $\binom{m}{r}$, and there are at most n possibilities for every single vertex. For the vertices we choose from the sets $B_i \cap C_i$ there are $\frac{2\lambda}{d}n$ possibilities.

Altogether we get the following upper bound for the number of such ordered sets:

$$\binom{m}{r} n^r \left(\frac{2\lambda}{d}n\right)^{m-r}.$$

By dividing by $m!$ to break up the order, and some calculations, we get the following upper bound for the number of unordered independent sets of $\mathcal{G}$ of size m:

$$\left(\frac{emd^2}{4\lambda n \log(n)}\right)^{\frac{2n\log(n)}{d}} \left(\frac{2e\lambda p}{md}\right)^m,$$

thus proving the lemma.

□

As we will discuss addition Cayley graphs of groups with prime order induced by sets $S \subseteq \mathbb{Z}_p$ of cardinality t, and thus t-regular, it will be convenient from now on to refer to (n, d, λ)-graphs as (p, t, λ)-graphs.

To use this result, we have to find out more about the eigenvalues of addition Cayley graphs, so as to find a good value for λ. Because of Theorem 3.5 we know that the absolute values of the eigenvalues of $A(Cay_G^+(S))$ are just the sums $\left|\sum_{s\in S}\chi(s)\right|$, where χ denotes a character of G.

As in our case $G = \mathbb{Z}_p$ and because these sums are in fact $\left|\sum_{s\in S}\omega^s\right|$, where ω is a non-trivial p-th root of unity. If we can find a good bound for $\left|\sum_{s\in S}\omega^s\right|$ then we can use this as our value for λ:

Lemma 3.23. *[Alo07] For every integer $t \leq p^{\frac{2}{3}}$ there exists a subset $S \subset \mathbb{Z}_p$ of cardinality t so that for every non-trivial p-th root of unity ω:*

$$\left| \sum_{s \in S} \omega^s \right| \leq 3\sqrt{t}\sqrt{\log(10p)}.$$

Proof. As the proof of this lemma uses arguments from probability theory that we do not want to deal with here, we refer to [Alo07].

□

With this estimate we can apply Lemma 3.21 to addition Cayley graphs:

Corollary 3.24. *[Alo07] There exists an addition Cayley graph $Cay^+_{\mathbb{Z}_p}(S)$ with $|S| = t = 9\frac{p^{\frac{2}{3}}}{\log^{\frac{1}{3}}(p)}$, that has at most*

$$e^{(2+o(1))p^{\frac{2}{3}}\log^{\frac{2}{3}}p}$$

independent sets.

Proof. Let $t = 9\frac{p^{\frac{2}{3}}}{\log^{\frac{1}{3}}(p)}$. According to Lemma 3.23 there is a subset $S \subset \mathbb{Z}_p$ of cardinality t such that for every non-trivial p-th root of unity ω:

$$\left| \sum_{s \in S} \omega^s \right| \leq 3\sqrt{t}\sqrt{\log(10p)}.$$

Therefore $Cay^+_{\mathbb{Z}_p}(S)$ is a (p, t, λ)-graph with $\lambda = 3\sqrt{t}\sqrt{\log(10p)}$. By Lemma 3.21 the number of independent sets of cardinality m in $Cay^+_{\mathbb{Z}_p}(S)$ for each $m \geq \frac{2p\log(p)}{t}$ is at most:

$$\left(\frac{emt^2}{4\lambda p \log(p)}\right)^{\frac{2p\log(p)}{t}} \left(\frac{2e\lambda p}{m}\right)^m.$$

This can be bounded by:

$$e^{\mathcal{O}\left(p^{\frac{1}{3}}\log^{\frac{7}{3}}(p)\right)} e^{(2+o(1))p^{\frac{2}{3}}\log^{\frac{2}{3}}(p)}$$

The number of independent sets of size $m \leq \frac{2p\log(p)}{t} = \mathcal{O}\left(p^{\frac{1}{3}}\log^{\frac{4}{3}}(p)\right)$ is at most $p^{\mathcal{O}\left(p^{\frac{1}{3}}\log^{\frac{4}{3}}(p)\right)}$ (which is a bound for all possible sets of size m). Summing over all values of m, we see that the number of independent sets of $Cay^+_{\mathbb{Z}_p}(S)$ is at most:

$$e^{(2+o(1))p^{\frac{2}{3}}\log^{\frac{2}{3}}(p)}$$

□

As motivated in the beginning of this section, we can use this upper bound on independent sets in $Cay^+_{\mathbb{Z}_p}(S)$ to prove Theorem 3.20:

Proof of Theorem 3.20. Let $S \subset \mathbb{Z}_p$ with cardinality t be as in Corollary 3.24. Set $t' = 7\frac{p^{\frac{2}{3}}}{\log^{\frac{1}{3}} p}$. There are:

$$\binom{p-t}{t'} = e^{(\frac{7}{3}-o(1))p^{\frac{2}{3}}\log^{\frac{1}{3}}(p)}$$

subsets S' of cardinality t' in $\mathbb{Z}_p - S$. As this number exceeds the number of independent sets A (see Corollary 3.24) in $Cay^+_{\mathbb{Z}_p}(S)$, it follows that there is a set S' such that there exists no independent set A in $Cay^+_{\mathbb{Z}_p}(S)$ for which $A + A = \mathbb{Z}_p - (S \cup S')$.

Suppose there is a non-independent set A in $Cay^+_{\mathbb{Z}_p}(S)$ such that $A+A = \mathbb{Z}_p-(S\cup S')$. Then $(A + A) \cap S = \emptyset$, which is a contradiction to A being non-independent. □

Theorem 3.20 shows us that addition Cayley graphs are not only interesting in themselves, but can also be used to give a rather easy and comprehensible proof to a complex additive combinatorial statement.

As very little is known about addition Cayley graphs, this proof uses properties of (n, d, λ)-graphs as a substitute (addition Cayley graphs are just a special case of the very general (n, d, λ)-graphs).

Using similar arguments as the ones applied here, it should be possible to find new results, or simplify some proofs of additive combinatorics.

However, before any of this can be done, many properties and graph-invariants of addition Cayley graphs need to be examined, to lay a solid foundation for further investigations.

In the next chapter we will deal with one of these graph properties, the Hamiltonicity.

4 Hamiltonicity of Cayley Graphs

In this chapter we will move away from additive combinatorics, and instead concentrate on one particular property of addition Cayley graphs, the Hamiltonicity.

In Section 4.1 we will give a short introduction to this problem and present a result for Cayley graphs over abelian groups.

Section 4.2 will deal with Hamiltonian circuits in addition Cayley graphs. In [CGW03] results are made to this end by restricting the set S to square-free sets. We will present some of those results and discuss the implications of the restriction to square-free sets.

In the final section we will drop the restriction to square-free sets and make some new results which yield Hamiltonian paths for a large class of addition Cayley graphs over cyclic groups. We will then use these Hamiltonian paths to motivate that the above mentioned conjecture can be improved to sets S of cardinality at least three, if $|G| \equiv 1 \mod 4$.

Throughout this chapter we will need the following notation:

Notation 4.1. Let $\mathcal{G}$ be a graph. In the following we will understand a *walk* W to be a sequence $(v_1, \ldots, v_k)$ such that $\{v_i, v_{i+1}\} \in E(\mathcal{G})$ for all $1 \leq i \leq k-1$. If, in addition to this, $v_i \neq v_j$ for all $1 \leq i, j \leq k$, $i \neq j$, we call W a *path*.

A *circle* will denote a closed walk, i.e. one where $v_1 = v_k$, and a closed path will be called a circuit (here we obviously have to allow $v_1 = v_k$ in the definition of path).

4.1 Hamiltonian Circuits in Cayley Graphs

The problem of finding Hamiltonian circuits in Cayley graphs was probably first studied by Rapaport-Strasser in an attempt to solve the "chess problem of the knight" in 1959 [RS59].

In 1969 Lovasz, inspired by a problem, which was posed by Gallai [Gal68], conjectured that every connected vertex-transitive graph contains a Hamiltonian path:

Conjecture 4.2. *(Lovász Conjecture)[Lov70] Every connected vertex-transitive graph contains a Hamiltonian path.*

This conjecture has still not been resolved.

Another conjecture though, that all connected vertex-transitive graphs with three or more vertices contain a Hamiltonian circuit, was soon discarded, as there are four counterexamples: the Petersen graph, the Coxeter graph, and the two graphs obtained from these by exchanging every vertex with a triangle [GM05].

Yet none of these graphs is a Cayley graph, giving rise to the following conjecture:

Conjecture 4.3. *[GM05] Every connected Cayley graph with three or more vertices contains a Hamiltonian circuit.*

Only partial progress has been made on this conjecture: For some groups the conjecture has been proved to be true and no counterexample has been found, but the full conjecture is far from being proved and there is some doubt that it is actually true.

For abelian groups the question is completely resolved:

Theorem 4.4. *[Mar83] Every connected Cayley graph of an abelian group of order at least three is Hamiltonian.*

Proof. This proof is based on [Mar83], but it has been strongly modified to make it more understandable and to avoid unnecessary notation.

We will prove this theorem using induction over $|S|$.

If $|S| = 1$, then $Cay(G, S)$ is not connected, as $|G| \geq 3$.

Let $|S| = 2$. As $Cay(G, S)$ is 2-regular and connected the graph just forms a Hamiltonian circuit.

Let $S > 2$. Then $S = \{s_1, \ldots, s_k\}$. Let $s \in S$, then $S' := S \backslash \{s, s^{-1}\}$. $Cay(\langle S' \rangle, S')$ is a connected Cayley graph.

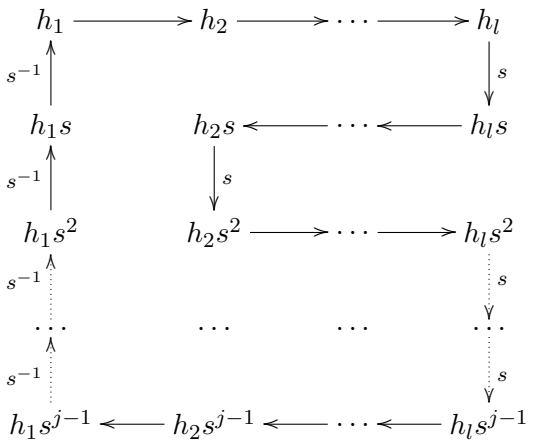
Suppose $|\langle S' \rangle| \geq 3$. Then by the induction hypotheses $Cay(\langle S' \rangle, S')$ is Hamiltonian and we can choose a Hamiltonian path $(h_1, \ldots, h_l)$, where $l := |\langle S' \rangle|$ and $h_i \in |\langle S' \rangle|$. If $\langle S' \rangle = G$, then we are done. Otherwise let j be the smallest integer such that $s^j \in \langle S' \rangle$.

Then $H, Hs, Hs^2, \ldots, Hs^{j-1}$ are all the cosets of H, they are all disjoint and their union is G. So for every coset of H we get a similar Hamiltonian path:

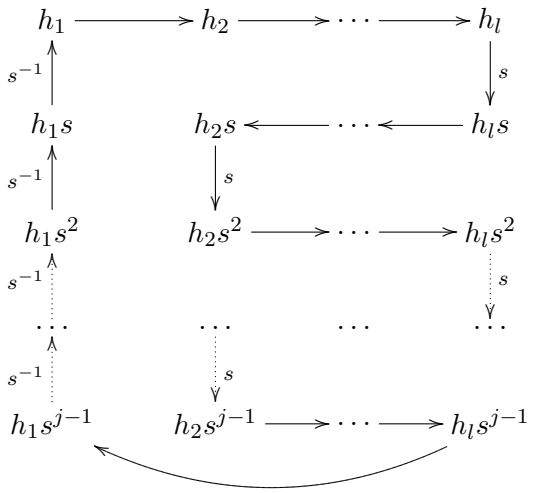
$$(h_1, \ldots, h_l);\ (h_1 s, \ldots, h_l s)\ ;\ \ldots\ ;\ (h_1 s^{j-1}, \ldots, h_l s^{j-1})$$

Now we join these paths together in the following order to get a Hamiltonian circuit:

If j is odd:



If j is even:



If $\langle S' \rangle < 3$, then S must be of the form $S = \{s_1, s_2, s_3\}$ with $s_1 = s_1^{-1}$ and $s = s_3 \neq s_2 = s^{-1}$. Then we can look at the set $S' := S \backslash \{s_1\}$. As $\langle S' \rangle \geq 3$ we can do the induction step as above.

□

As the question of Hamiltonicity in Cayley graphs has received so much attention in literature, it is natural to ask the same question for addition Cayley graphs; i.e. is every connected addition Cayley graph with three or more vertices Hamiltonian?

As addition Cayley graphs are only defined over abelian groups and we have just seen that for standard Cayley graphs over abelian groups the question is quickly resolved, there seems to be some hope that this might be easily answered.

However, addition Cayley graphs are not vertex transitive, not even necessarily regular, disqualifying them even for the Lovasz conjecture.

In fact, there is a simple counterexample to the statement, even for sets S of cardinality three, as can be seen in Figure 4.1.

The question remains whether it is possible to restrict the group G or the set S in any way to gain Hamiltonicity.

In the next section we will present some results made in [CGW03] by restricting the set S to square-free sets (sets without elements of the form $s = h + h$, $h \in G$). While these results are quite conclusive, the restriction to square-free sets is very strong and discounts most of the possible addition Cayley graphs.

In [Lev10] V. Lev comes to the conclusion that for any Hamiltonian addition Cayley graph $Cay_G^+(S)$ we have:

$$|S| \geq rk(G),$$

where $rk(G)$ denotes the minimum cardinality of a generating set of G.

This suggests that we have to look at groups with small generating sets to gain interesting results on the Hamiltonicity of addition Cayley graphs.

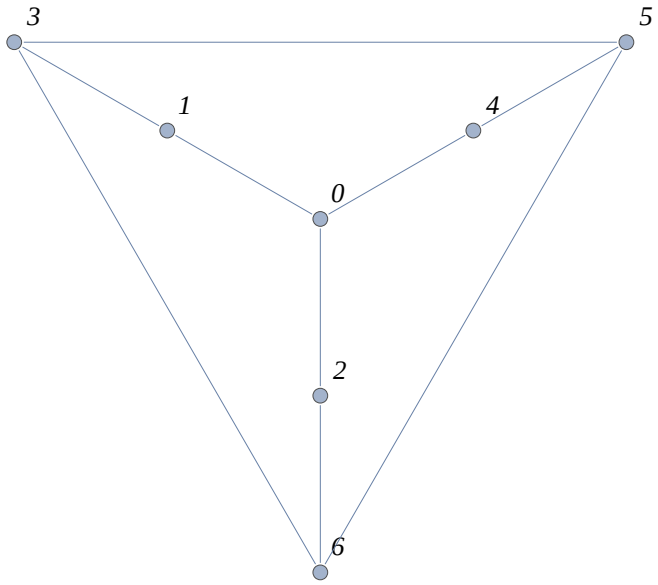


Figure 4.1: $Cay^+_{\mathbb{Z}_7}(\{1,2,4\})$ without self loops

The most natural type of group fulfilling this criterion are obviously cyclic groups.

It is easy to see that the cardinality of S must be at least two for there to be any kind of circuit at all. The example previously shown furnishes us with a non-Hamiltonian addition Cayley graph over a cyclic group with $|S| = 3$.

E. Croot and V. Lev give the following conjecture in [CL]:

Conjecture 4.5. *[CL] Let G be a finite cyclic group and S a subset of G of cardinality at least four, such that $Cay^+_G(S)$ is connected. Then $Cay^+_G(S)$ is Hamiltonian.*

This conjecture is still open and, as motivated above, is best-possible for arbitrary cyclic groups.

In the next two sections we will present some of the results on the Hamiltonicity of addition Cayley graphs already mentioned, and then attempt to make some progress toward this conjecture.

4.2 Addition Cayley Graphs over Square-Free Sets

We begin with the following definition:

Definition 4.6. (square) Let G be an abelian group and $g \in G$. Then we will call g a *square*, if there is $h \in G$ such that $g = h + h$; we will call h a root of g. A *square-free subset* of G will therefore be a subset not containing any squares.

If we restrict the set S from the definition of addition Cayley graphs to square-free sets, we ensure that there are no self-loops in $Cay^+_G(S)$, thus making the graph $|S|$-regular.

Addition Cayley graphs of this form are more similar to regular Cayley graphs, in fact connected bipartite addition Cayley graphs over square free sets are in fact nothing other than regular Cayley graphs [CGW03]. This makes the search for Hamiltonian circuits somewhat easier and in the following we will present some of the possible results. More on this subject can be found in [CGW03].

For this section we will need the following notation for paths (and walks):

Notation 4.7.

- Let $P_1 := (v_1, \ldots, v_m)$ and $P_2 := (v_m, \ldots, v_n)$ be paths in a graph $\mathcal{G}$. Then $P_1 * P_2$ is the path $(v_1, \ldots, v_m, v_{m+1}, \ldots, v_n)$.
- Let G be an abelian group and $S \subseteq G$. For $g \in G$ and $s_1, \ldots, s_n \in S$ we denote by $(g; s_1 s_2 \ldots s_n)$ the path $(v_0, \ldots, v_n)$ in $Cay_G^+(S)$ where $v_0 := g$ and $v_i := s_i - v_i$ for $i \in \{1, \ldots n\}$.

To find Hamiltonian circuits and paths in addition Cayley graphs we will first need a better understanding of what a path and a circuit (walks and circles behave in the same way) in the graph actually imply for the elements of the group. To illustrate this we begin with a path of length 2 (Figure 4.2).

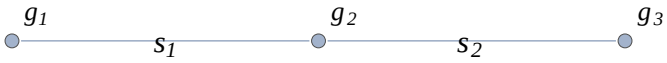


Figure 4.2: Path of length 2

As $g_1 + g_2 = s_1$ and $g_2 + g_3 = s_2$ we get $g_1 - g_3 = s_1 - s_2$. If we iterate this principle for a path of even length l we get:

$$g_1 - g_{l+1} = s_1 - s_2 + s_3 - \ldots + s_{l-1} - s_l.$$

For a path of odd length say 3 we get a slightly different picture (Figure 4.3).

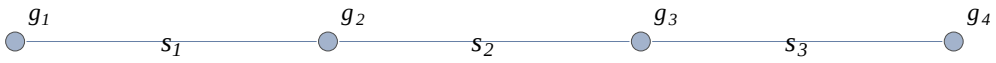


Figure 4.3: Path of length 3

As above we have $g_1 + g_2 = s_2$, $g_2 + g_3 = s_2$ and $g_3 + g4 = s_3$. Computation yields $g_1 + g_4 = s_1 - s_2 + s_3$, and thus by iteration we receive for odd length l:

$$g_1 + g_l = s_1 - s_2 + s_3 - \ldots - s_{l-1} + s_l.$$

If we view a circuit in the graph as a path from a given vertex g to itself, the above equations yield:

$$0 = s_1 - s_2 + s_3 - \ldots + s_{l-1} - s_l,$$

for a circuit off even length l, and:

$$g + g = 2g = s_1 - s_2 + s_3 - \ldots - s_{l-1} + s_l,$$

for a circuit of odd length l.

All of the above disregards the existence of loops which appear in many addition Cayley graphs. As they will sometimes be useful to simplify the notation, we will not completely disregard self-loops, but be consciously ambivalent, so as to be able to use them, when they are needed. In this section none of the graphs will contain self-loops, as we are dealing with square free sets, but in the next section they will play an important role.

Using a square-free subset of G to construct an addition Cayley graph we get a stronger characterisation of bipartition:

Proposition 4.8. *[CGW03] Let G be an abelian group and S a square-free subset of G such that $Cay^+_G(S)$ is connected. Then the following statements are equivalent:*

i) $Cay^+_G(S)$ is bipartite

ii) S is contained in the non-zero coset of an index 2 subgroup of G, but not contained in any other coset (especially $|\langle S - S\rangle| = \frac{|G|}{2}$).

Proof. *ii)* $\Rightarrow$ *i)* is a special case of Proposition 3.4.

Suppose $Cay^+_G(S)$ is bipartite. Then $G = A \cup B$ such that $E\left(Cay^+_G(S)\right) = \{\{a, b\} : a \in A, b \in B\}$. We can assume that $0 \in A$.

As $Cay^+_G(S)$ is connected, one of the following must hold:

1. S is not contained in a coset of a proper subgroup of G, or
2. S is contained in the non-zero coset of an index 2 subgroup of G, but not in any other coset.

Suppose (1) holds. Then $\langle S - S\rangle = G$. Let $b \in B$. Then we can write b as:

$$b = (s_1 - s_2) \pm (s_3 - s_4) \pm \ldots \pm (s_{k-1} - s_k),$$

with k even and $s_1, \ldots, s_k \in S$. As G is abelian, we can rewrite this equation as:

$$b = s'_1 - s'_2 + s'_3 - s'_4 + \ldots + s'_{k-1} - s'_k.$$

This implies that there is a path of even length between 0 and b, which is a contradiction to $Cay^+_G(S)$ being bipartite. Thus we get 2).

□

From now on we will only be interested in cubic addition Cayley graphs, i.e. over square-free sets of cardinality three.

In this case we can give an alternative characterisation of bipartition:

Proposition 4.9. *[CGW03] Let G be a group and $S = \{s_1, s_2, s_3\}$ a square-free subset of G of cardinality three. Then $Cay^+_G(S)$ is bipartite if and only if $s_1 + s_2 + s_3$ is a square.*

Proof. Suppose $s_1 + s_2 + s_3 = 2g$ is a square. Then the vertices $g_1 = g - s_1$, $g_2 = g - s_2$ and $g_3 = g - s_3$ form a triangle. Thus Cay^+_G is not bipartite, as bipartite graphs do not contain odd circuits.

Suppose $Cay^+_G(S)$ is not bipartite. Then it contains an odd circuit, $(g_0, g_1, \ldots, g_n = g_0)$.

For $1 \leq i \leq n$, let $a_i = g_{i-1} + gi$. Obviously all the a_i are elements of S. As we have an odd circuit, there exists a $g \in G$ with:

$$2g = a_1 + a_2 + \ldots + a_n = ks_1 + ls_2 + ms_3,$$

where $k + l + m = n$ is odd.

Supposing that two of these numbers are even, for instance l and k, we see that:

$$s_3 = 2g - ks_1 - ls_2 - (m-1)s_3$$

is a square, which is a contradiction.

Thus k, l and m are odd and:

$$s_1 + s_2 + s_3 = g - (k-1)s_1 - (l-1)s_2 - (m-1)s_3$$

is a square, proving the statement.

□

With these statements in mind we can move to the first result on Hamiltonicity:

Theorem 4.10. *[CGW03] Let G be an abelian group with $|G| \equiv 0 \mod 4$ and let S be a square-free subset of G of cardinality three. If $Cay^+_G(S)$ is connected and bipartite, then it is Hamiltonian.*

Why the unusual condition $|G| \equiv 0 \mod 4$ is necessary, will be made clearer by the proof. But just claiming that the graph is bipartite, by Proposition 4.8 implies that $|G|$ is divisible by 2.

For the proof of this theorem we first need the following technical lemma:

Lemma 4.11. *[CGW03] Let G_1 be an abelian group of odd order and let G_2 be a non-trivial abelian 2-group. Let $G := G_1 \times G_2$ and S a square-free subset of G of cardinality three. If either of the following holds:*

i) G_2 is not isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_2^2$,

ii) G_2 is isomorphic to $\mathbb{Z}_2^2$ and the sum of the three elements of S is a not square,

then there exist distinct $s_1, s_2 \in S$ such that $(G : \langle s_1 - s_2 \rangle) \equiv 0 \mod 4$.

Proof. Let $G_1 = H_1 \times \ldots \times H_l$, where H_i is a cyclic group of order 2^{k_i} with $1 \leq k_1 \leq \ldots \leq k_l$.

Every $g \in G$ has order $2^k \cdot m$ with $0 \leq k \leq k_l$ and m odd. Therefore, if $s \geq 3$ or $l = 2$ and $k_1 \geq 2$, then $(G : \langle g \rangle) \equiv 0 \mod 4$ for every $g \in G$.

Thus there are only three special cases left to clarify:

1. $l = 2$, $k_1 = 1$ and $k_2 \geq 2$.

   We represent every $g \in G$ as $g = (g_0, g_2, g_3)$ with $g_0 \in G_0$, $g_1 \in \{0, 1\}$, and $g_2 \in \{0, 1, \ldots, 2^{k_2} - 1\}$. Among any three elements of G, one can choose two whose last components are of the same parity. If s_1 and s_2 are such elements, then $|\langle s_1 - s_2 \rangle|$ divides $2^{k_1 - 1} \cdot |G_0|$, and therefore $(G : \langle s_1 - s_2 \rangle) \equiv 0 \mod 4$.

2. $l = 2$, $k_1 = k_2 = 1$ and the sum of the three elements of $S = \{s_1, s_2, s_3\}$ is not a square.

   We represent every $g \in G$ as $g = (g_0, g_1, g_2)$ with $g_0 \in G_0$ and $g_1, g_2 \in \{0, 1\}$. As a, b, c and $a + b + c$ are not squares, at least one of the two last elements of each of these has to be equal to 1. This implies that $|\langle s_1 - s_2 \rangle|$ is odd and therefore that $(G : \langle s_1 - s_2 \rangle) \equiv 0 \mod 4$.

3. $s = 1$ and $k_1 \geq 2$

   We represent every $g \in G$ as $g = (g_1, g_2)$ with $g_0 \in G_0$ and $g_2 \in \{0, 1, \ldots, 2^{k_1} - 1\}$. As the three elements of S are not squares, their last components are odd. Therefore one can chose two elements of S, s_1 and s_2, whose second components are congruent modulo 4. Then $|\langle s_1 - s_2 \rangle|$ divides $2^{k_1 - 2} \cdot |G_0|$ resulting in $(G : \langle s_1 - s_2 \rangle) \equiv 0 \mod 4$.

□

Proof of Theorem 4.10. Let $S = \{s_1, s_2, s_3\}$ be square free, such that $Cay_G^+(S)$ is a connected bipartite graph. Then $|\langle S - S \rangle| = \frac{|G|}{2}$. By Lemma 4.11 we know that $(G : \langle s_1 - s_2 \rangle) = 2n$, where n is even. Let $m := |\langle s_1 - s_2 \rangle|$. Therefore $|G| = 2nm$.

It is easy to see, that:

$$|\langle S - S \rangle| = \langle s_1 - s_2, s_1 - s_3 \rangle,$$

both of cardinality nm. This implies that $n(s_3 - s_1) \in \langle s_2 - s_1 \rangle$ and hence:

$$\frac{n}{2}(2s_3 - s_1 - s_2) = n(s_3 - s_1) + \frac{n}{2}(s_1 - s_2) \in \langle s_2 - s_1 \rangle.$$

We then know that there exists a $q \in \{0, \ldots, m - 1\}$ such that:

$$\frac{n}{2}(2s_3 - s_1 - s_2) = q(s_2 - s_1).$$

We will now construct a circle in $Cay_G^+(S)$ and then show that this is in fact a Hamiltonian circuit.

The first thing we need to do, is split the group G up into easily manageable subsets, which will later enable us to check our circle for Hamiltonicity.

Let Γ_{s_1,s_2} be the graph with vertex set:

$$V(\Gamma_{s_1,s_2}) = G/\langle s_1 - s_2\rangle,$$

and edge set:

$$E(\Gamma_{s_1,s_2}) = \{\{\pi(x), \pi(y)\} : \pi(x) + \pi(y) \in \pi(S), \pi(x) \neq \pi(y)\},$$

where π is the natural injection from G to $G/\langle s_1 - s_2\rangle$.

As $Cay^+_G(S)$ is connected, it is easy to see that Γ_{s_1,s_2} is connected.

This graph has maximum degree two, as $\pi(s_1) = \pi(s_2)$. Suppose $\pi(s_1)$ is a square. Then $s_1 = 2u+k(s_1-s_2)$, where $u \in G/\langle s_1 - s_2\rangle$ and $k \in \mathbb{Z}$ is odd (as s_1 is not a square). This implies that $s_2 = 2u + (k-1)s_1 - (k-1)s_2$ is square, which is a contradiction.

Suppose $\pi(s_3)$ is a square. Again we get $s_3 = 2u + k(s_1 - s_2)$ with $k \in \mathbb{Z}$ is odd. This implies that $s_1 + s_2 + s_3 = 2u + (k-1)s_1 - (k-1)s_2$ is a square, which is contradiction to $Cay^+_G(S)$ being bipartite due to Proposition 4.9.

Thus $\pi(S)$ is square free making Γ_{s_1,s_2} a connected 2-regular graph, i.e. a circuit of length $2n$. By $X_1, Y_1, \ldots, X_n, Y_n$ we denote the consecutive vertices of Γ_{s_1,s_2}, such that $X_1 + Y_1 = \pi(s_1)$. We use capitals for these vertices to emphasise that they are also sets of elements of G. Also we can see that:

$$X_1 \cup Y_1 \cup \ldots \cup X_n \cup Y_n = G. \tag{4.1}$$

Let $d := \gcd(q, m)$, $m = pd$ and $x \in X_1$. For $i \in \{0, \ldots, p-1\}$ we set $z_i := x + iq(b-a)$. The circle we want to construct will consist of $s-1$ consecutive walks $P(z_i)$, defined as:

$$P(z_i) := \left(z_i; \left((s_2s_1)^{d-1}s_2s_3\right)^{\frac{n}{2}} \left((s_1s_2)^{d-1}s_1s_3\right)^{\frac{n}{2}}\right)$$

Every one of these walks visits alternating $2(d-1)$ vertices in X_1 and Y_1 using s_1- and s_2-edges, to then take a s_3-edge to X_2 and Y_2. This goes on until we are in X_n and Y_n, where the last s_3 edge takes us back to X_1.

It remains to show that $P(z_0) * P(z_1) * \ldots P(z_{p-1})$ is a Hamiltonian circuit.

First we need to show that the last vertex of every $P(z_{i-1})$, say $v(z_{i-1})$, is the first vertex of every $P(z_i)$ for $i \in \{1, \ldots, p-1\}$, and that the last vertex of $P(z_{p-1})$ is the first vertex of $P(z_0)$.

Calculating the $v(z_{i-1})$ and $v(z_{p-1})$we get:

$$v(z_{i-1}) = z_{i-1} + \frac{n}{2}(2s_3 - s_1 - s_2) = z_{i-1} + q(s_2 - s_1) = z_i,$$

and

$$v(z_{p-1}) = z_{p-1} + q(s_2 - s_1) = x + pq(s_2 - s_1) = x = z_0,$$

because $s_2 - s_1$ has order m. Thus $P(z_0) * P(z_1) * \ldots P(z_{p-1})$ is a circle in $Cay^+_G(S)$.

To prove that it is Hamiltonian we need to show that every vertex in this circle is distinct.

Let $u_j(z_i)$ be the first vertex of $P(z_i)$ that is in X_j. Then $u_1(z_i) = z_i$, and for $2 \leq j \leq n$ we have:

$$u_j(z_i) := \begin{cases} u_{j-1}(z_i) + (d-1)(s_1 - s_2) + s_3 - s_2, & \text{if } j \leq \frac{n}{2} + 1 \\ u_{j-1}(z_i) + (d-1)(s_2 - s_1) + s_3 - s_1, & \text{if } j > \frac{n}{2} + 1 \end{cases}$$

For $z_i, z_{i+1} \in X_1$ this implies that:

$$u_j(z_i) - u_j(z_{i+1}) = z_i - z_{i+1}.$$

Let $V(z_i)$ denote all vertices of $P(z_i)$ excluding the last one. Then the following equations hold:

$$V(z_i) \cap X_j = \begin{cases} \{u_j(z_i) + l(s_1 - s_2) : 0 \leq l \leq d-1\}, & \text{if } j \leq \frac{n}{2} \\ \{u_j(z_i) + l(s_1 - s_2) : 0 \leq l \leq d-1\}, & \text{if } j > \frac{n}{2} \end{cases},$$

and

$$V(z_i) \cap Y_j = \begin{cases} s_2 - (V(z_i) \cap X_j), & \text{if } j \leq \frac{n}{2} \\ s_1 - (V(z_i) \cap X_j), & \text{if } j > \frac{n}{2} \end{cases}.$$

These equations imply that all vertices in a given $V(z_i)$ are distinct and that $V(z_i) \cap V(z_{i+1}) = \emptyset$, for all $0 \leq i < p-1$, as $z_i - z_{i+1} = s_1 - s_2$.

Finally we know that:

$$\sum_{i=0}^{p-1} |V(z_i)| = p|V(z_0)| = p \cdot 2nd = 2mn = |G|,$$

proving that $P(z_0) * P(z_1) * \ldots P(z_{p-1})$ is a Hamiltonian circuit.

□

If we claim that $|G| \equiv 0 \mod 8$ we can show a similar statement for non-bipartite graphs. In the proof we will explain, why this added requirement is necessary.

Theorem 4.12. *[CGW03] Let G be an abelian group with $|G| \equiv 0 \mod 8$ and let S be a square-free subset of G of cardinality three. If $Cay_G^+(S)$ is connected, then it is Hamiltonian.*

Proof. Let $S = \{s_1, s_2, s_3\}$ be square free such that $Cay_G^+(S)$ is a connected graph. Because of Theorem 4.10 we can assume that $Cay_G^+(S)$ is not bipartite and thus, because S square free, that $s_1 + s_2 + s_3$ is a square. Applying Lemma 4.11 we know that $(G : \langle s_1 - s_2 \rangle) = 2n$, where n is even. Let $m := |\langle s_1 - s_2 \rangle|$.

As in Theorem 4.10 we construct the graph Γ_{s_1,s_2} and as in Theorem 4.10 we see that $\pi(s_1)$ is not a square. However, as the graph is bipartite, and thus $s_1 + s_2 + s_3$ is a square, we see that $\pi(s_3)$ in this case is in fact a square.

As a result, Γ_{s_1,s_2} this time takes the shape of a path, as it is connected but not 2-regular. We denote this path as $X_1, Y_1, \ldots, X_n, Y_n$, and because $\pi(s_3)$ is a square $X_1 + Y_1 = \pi(s_1)$.

Every element of X_1 is connected by a s_3-edge to another element of X_1 in $Cay^+_G(S)$ and therefore $|X_1| = m$ is even. This fact motivates why $|G|$ is assumed to be divisible by 8, as opposed to 4 in Theorem 4.10.

Because $Cay^+_G(S)$ is not bipartite, $\langle S - S\rangle = \langle s_1 - s_2, s_1 - s_3\rangle = G$ and thus is of cardinality $2nm$. This also implies that $|\langle s_1 - s_3\rangle| = 2n$ and:

$$n(2s_3 - s_1 - s_2) = 2n(s_3 - s_1) + n(s_1 - s_2) = n(s_1 - s_2) \in \langle s_1 - s_2\rangle .$$

We know that there exists a $q \in \{0, \ldots, m-1\}$ such that:

$$n(2s_3 - s_1 - s_2) = q(s_2 - s_1).$$

Then $q \equiv n \mod m$ and is therefore even. Let $d = \gcd(q, m)$ (so $d \geq 2$) and $m = dp$. We define the walks $P(z_i)$ for $i \in \{0, \ldots, p-1\}$ as follows:

$$P(z_i) := (z_i; w_1, \ldots, w_{2n}) ,$$

where

$$w_j := \begin{cases} s_2 s_3, & \text{if } j \leq n \text{ and } j \text{ is odd,} \\ s_1 s_3, & \text{if } j \leq n \text{ and } j \text{ is even,} \\ (s_1 s_2)^{d-2} s_1 s_3, & \text{if } j > n \text{ and } j \text{ is odd,} \\ (s_2 s_1)^{d-2} s_2 s_3, & \text{if } j > n \text{ and } j \text{ is even.} \end{cases}$$

As in Theorem 4.10 the Hamiltonian circuit will be the conjunction of these walks. However, proving that the walks are disjunct, although very similar, is much more intricate, which is why we refer to [CGW03] for the rest of the proof.

□

Although the results from this section seem rather satisfying and conclusive (in [CGW03] the bipartite case is even nearly completely resolved), they are strongly restricted by their setting.

Not only are all addition Cayley graphs over non-square-free sets disregarded, we have also restricted ourselves to groups of even order as a result of the strong reliance on bipartition (which with square free sets implies a group of even order).

Therefore, in the next section we will examine whether any results are possible if we leave the setting of square-free sets.

4.3 The Hamiltonicity of addition Cayley graphs over cyclic groups

In the last section, we discussed the Hamiltonicity of addition Cayley graphs under the assumption that the underlying set S is square-free. This assumption results in the graph containing no loops and thus being strictly regular.

This assumption though is, of course, very restrictive, as most subsets of groups will contain at least one square.

On the other hand, if we drop this assumption we get small and easy counterexamples of addition Cayley graphs over sets of cardinality 3, which are biconnected but not Hamiltonian; for example $Cay^+_{\mathbb{Z}_7}$ with $S = \{1, 2, 4\}$(Figure 4.4).

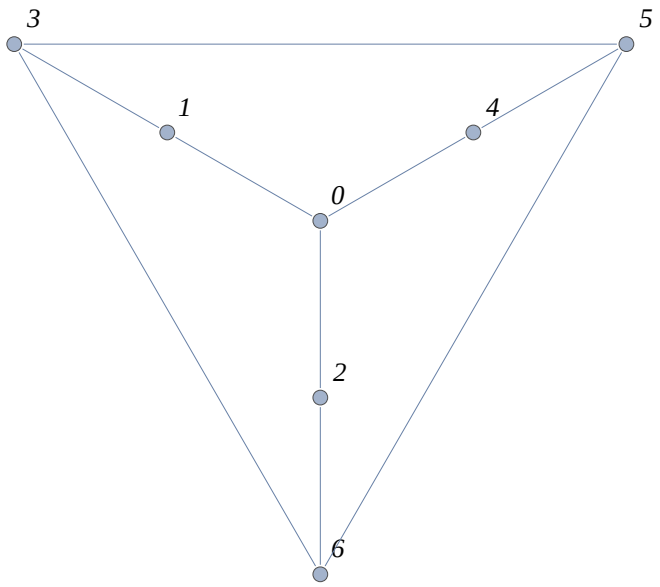


Figure 4.4: $Cay^+_{\mathbb{Z}_7}(\{1, 2, 4\})$ without self loops

This graph is not Hamiltonian because the vertex 0 is connected to all three vertices of degree 2, namely 1, 2, and 4, making a Hamiltonian circuit impossible.

To make any kind of plausible conjecture concerning Hamiltonicity over general addition Cayley graphs, we will have to restrict ourselves to a particular type of group, so as to be able to determine the amount of squares in our set S.

The easiest type of abelian group is a cyclic group, and already in this setting the only statement in the literature (apart from [Lev10], which is in a completely different vein) is the following conjecture:

Conjecture 4.13. *[CL] Let G be a finite cyclic group and S a subset of cardinality at least 4 such that $Cay^+_G(S)$ is connected. Then $Cay^+_G(S)$ is Hamiltonian.*

The question arises, why the set S has to be of cardinality 4 as opposed to 3, as in the last section.

There are two reasons for this: Firstly if S were to be of cardinality 3 and one of its elements a square, the graph would be less than cubic, and for a graph to be at least cubic is an assumption often used in regard to Hamiltonicity.

The other (and decisive) reason is the existence of counterexamples.

Above we have already given one example of an addition Cayley graph over a cyclic group and a set of cardinality 3, which is not Hamiltonian. Furthermore in [Lev10] it is stated that "it can be shown that if $n \equiv 3 \mod 4$, $G = \mathbb{Z}_n$, and $S = \{0, 1, 3\} \subseteq G$ (Figure 4.5), then $Cay_G^+(S)$ is 2-connected, but not Hamiltonian"; a fact that we will examine further on.

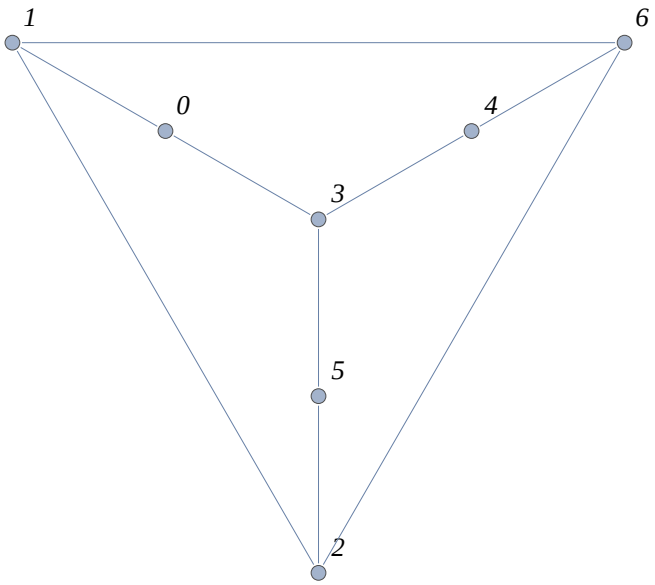


Figure 4.5: $Cay_{\mathbb{Z}_7}^+(\{0, 1, 3\})$without self-loops

As already mentioned, the number of squares in S and thus the number of self-loops in $Cay_G^+(S)$ will be very important in determining whether $Cay_G^+(S)$ is Hamiltonian.

For cyclic groups this question is quickly answered:

Proposition 4.14. *Let G be a cyclic group.*

i) If G is of odd order, then every element of G is a square and has a unique root.

ii) If G is of even order, then all elements of G that are squares are contained in the unique subgroup of index 2, and have exactly two roots.

This proposition suggests that it is convenient to treat the case of odd-order groups separately from that of even-order groups.

While addition Calyey graphs over cyclic groups of odd order will always have $|S|$ self-loops, the even order case is more complicated. Thus, from now on we will only be interested in cyclic groups of odd order.

Lemma 4.15. *Let G be a cyclic group of odd order. Let $S = \{s_1, s_2\}$ be a subset of G with cardinality 2, then $Cay_G^+(S)$ consists of one path and circuits, which are pairwise vertex-disjoint.*

Let m denote the period of $s_1 - s_2$. Then the length of the path is $m-1$, leads from the root of s_1 to the root of s_2. The length of a circuit is $2m$.

Proof. As G has odd order, every element of G is a square. Thus there are $g_1, g_2 \in G$ such that $s_1 = g_1 + g_1$ and $s_2 = g_2 + g_2$.

Every vertex of $Cay_G^+(S)$ has degree 2, while g_1 and g_2 have degree 1. Therefore the graph must consist of one path from g_1 to g_2 and circuits otherwise. Also for reasons of degree, the circuits and the path must be pairwise vertex-disjoint.

As m is the period of $s_1 - s_2$ we get:

$$2g_1 + 2g_2 = s_1 - s_2 = (m+1)(s_1 - s_2).$$

As G has odd order, m must be odd. Therefore the above can be written as:

$$g_1 - g_2 = \frac{m+1}{2}(s_1 - s_2). \tag{4.2}$$

The path from g_1 to g_2 must have alternating s_1- and s_2-edges, where g_1 is incident to a s_2-edge and g_2 incident to a s_1-edge.

Now if l describes the length of the path (l is obviously even), by using the s_1-loop we get the equation:

$$g_1 - g_2 = \frac{l+2}{2}(s_1 - s_2).$$

Because m is the period of $s_1 - s_2$ we see that $m - 1 \leq l$.

On the other hand, we can construct a walk from Equation 3.2 which has length $m-1$, implying that the path does in fact have exactly length $m-1$.

To calculate the length of a circuit, we must choose one of its vertices g. As g is an element in a circuit, there must be a path from g to itself; this path must have alternating s_1 and s_2 edges and must w.l.o.g begin with an s_1-edge and end in an s_2 edge (and thus is of even length).

From these observations we get the following equation:

$$0 = \frac{l}{2}(s_1 - s_2),$$

where l denotes the length of the circuit.

Hence $\frac{l}{2}$ must be a multiple of m, as m is the period of $s_1 - s_2$. Like above, this suffices to show that l is in fact exactly $2m$.

□

A useful result of this lemma is the following corollary:

Corollary 4.16. *Let G be a cyclic group of odd order and S a subset of G.*

If S contains a pair of elements s_1, s_2 such that $\langle s_1 - s_2 \rangle = G$, then $Cay_G^+(S)$ contains a Hamiltonian path.

Proof. This is an easy consequence of Lemma 4.15.

□

Using this corollary we can even make a stronger statement for addition Cayley graphs over sets S with cardinality at least two:

Lemma 4.17. *Let G be a cyclic group of odd order. Let $S = \{s_1, \ldots, s_{2m}\}$ be a subset of even cardinality such that $Cay_G^+(S)$ is connected and such that $s_1 - s_2, s_3 - s_4, \ldots, s_{2m-1} - s_{2m}$ all generate G (after appropriate reordering).*

Then the edge set of $Cay_G^+(S)$ can be partitioned into m pairwise edge-disjoint Hamiltonian paths.

Proof. Consider $Cay_G^+(\{s_1, s_2\}), \ldots, Cay_G^+(\{s_{2m-1}, s_{2m}\})$. Everyone of these graphs is a subgraph of $Cay_G^+(S)$ and because of Corollary 3.24 they are all Hamiltonian paths. □

For groups of prime order, a connected addition Cayley graph will thus always contain a Hamiltonian path. For cyclic groups in general this has not been shown yet. But computations by the author suggest that the following conjecture is true:

Conjecture 4.18. *Let G be a cyclic group of odd order, an S a subset of cardinality 3 such that $Cay_G^+(S)$ is connected. Then $Cay_G^+(S)$ contains a Hamiltonian path.*

What these computations are, and why they are convincing will be explained when we introduce Conjecture 4.23.

On the other hand, connected addition Cayley graphs over p-groups will always contain a Hamiltonian path:

Proposition 4.19. *Let G be a cyclic p-group of odd order, i.e. $|G| = p^m$. Let S be a subset of G, such that $Cay_G^+(S)$ is connected, then $Cay_G^+(S)$ contains a Hamiltonian path.*

Proof. Let $S = \{s_1, \ldots, s_k\}$. Suppose that for all $1 \leq i, j \leq k$ $s_i - s_j$ does not generate G. Then for all $1 \leq i, j \leq k$ there is a subgroup of G, namely H_{ij}, such that $s_i - s_j \in H_{ij}$.

As G is a p-group, all subgroups of G are contained in the unique subgroup of order p^{m-1} which we define as H^*. Therefore for every $1 \leq i, j \leq k$ we have $s_i - s_j \in H^*$.

As a consequence we get:

$$H^* + s_1 = H^* + s_2 + \ldots + H^* + s_k.$$

This implies that S is a subset of $H^* s_1$, and thus that $Cay_G^+(S)$ is not connected.

As this is a contradiction, there must be a pair of elements whose difference generates G. According to Corollary 3.24, $Cay_G^+(S)$ must contain a Hamiltonian path. □

The next step will be to use these Hamiltonian paths to construct a Hamiltonian circuit. Because the Hamiltonian circuit problem is even NP-complete when we are given a Hamiltonian path, it is not immediately clear how this information can help, but the Hamiltonian paths will give us an insight on the rather symmetric structure of graphs over groups of prime order.

Before moving on to Conjecture 4.13 we will first consider addition Cayley graphs, where G is cyclic of odd order, and S has cardinality 3.

As we have seen in Corollary 4.16, $Cay_G^+(s)$ will contain a Hamiltonian path if there is a pair $s_i, s_j \in S$ such that $s_i - s_j$ is a generator of G. If G is of prime order, every element is a generator, and we can take a Hamiltonian path for granted. Thus the case of $|G|$ prime seems to be the best place to start.

As G cyclic of prime order p is isomorphic to $\mathbb{Z}_p$, it is a field and every element has a multiplicative inverse. If in the following we make any calculations with elements of such a G these are meant to be performed in the field arithmetic, and if $1, 2, 3 \ldots$ are used in these calculations we will mean elements of $\mathbb{Z}_p$.

Lemma 4.20. *Let G be a cyclic group of order p, where p is an odd prime, and $S = \{s_1, s_2, s_3\}$ and $S' = \{s_1', s_2', s_3'\}$ subsets of G of order 3.*

Then $Cay_G^+(S)$ and $Cay_G^+(S')$ are isomorphic if and only if there is an ordering of S and S' such that:

$$\frac{s_3 - s_2}{s_1 - s_2} = \frac{s_3' - s_2'}{s_1' - s_2'}.$$

Proof. As $s_1 - s_2$ generates G, there is a Hamiltonian path from the root of s_1 to the root of s_2 in $Cay_G^+(S)$, namely $P = (g_1, \ldots, g_p)$.

As $s_1' - s_2'$ also generates G we get a Hamiltonian path from the root of s_1' to the root of s_2' in $Cay_G^+(S')$, namely $P' = (g_1', \ldots, g_p')$.

To get the desired isomorphism from $Cay_G^+(S)$ to $Cay_G^+(S')$ we map g_i to g_i' for all $1 \leq i \leq p$.

For this map to be an isomorphism the following must hold:

$$\{g_i, g_j\} \in E\left(Cay_G^+(S)\right) \Leftrightarrow \{g_i', g_j'\} \in E\left(Cay_G^+(S')\right),$$

for all $1 \leq i, j \leq p$.

For all s_1 and s_2 edges this is true, as we are mapping the two Hamiltonian paths containing all s_1- and s_2-edges upon each other.

Thus it is sufficient to show:

$$g_i + g_j = s_3 \Leftrightarrow g_i' + g_j' = s_3',$$

for all $1 \leq i, j \leq p$.

So let $g_i + g_j = s_3$ and $l := \frac{s_3 - s_2}{s_1 - s_2}$. Then we get $g_i + g_j = l(s_1 - s_2) + s_2$. This implies a walk from g_i to g_j along the Hamiltonian path P.

As we projected P onto P' we have an equivalent walk from g_i' to g_j' along P', which implies that $g_i' + g_j' = l(s_1' - s_2') + s_2' = s_3'$ and hence proves the statement.

□

This lemma implies that for G of prime order there are only few different addition Cayley graphs, as most of these are isomorphic. At first glance it seems that there are

$p-2$ different graphs, one for each value of $\frac{s_3-s_2}{s_1-s_2}$ apart from 0 and 1 (which both imply that $s_i = s_j$ for some $1 \leq i, j \leq 3$). In fact, there are even less possibilities than this.

For convenience sake we make the following definition:

Definition 4.21. (ratio) Let G be a cyclic group of order p, where p is an odd prime, and $S = \{s_1, s_2, s_3\}$ a subset of G of cardinality 3.

Then we define:

$$r\left(Cay_G^+(S)\right) = \frac{s_3 - s_2}{s_1 - s_2}$$

to be the *ratio* of $Cay_G^+(S)$.

Obviously the ratio of $Cay_G^+(S)$ depends on the ordering of the three elements of S and is thus not uniquely defined.

If we set r to be the ratio of $Cay_G^+(S)$ we get the following equations:

- $\frac{s_3-s_2}{s_1-s_2} = r$
- $\frac{s_1-s_2}{s_3-s_2} = \frac{1}{r}$
- $\frac{s_3-s_1}{s_2-s_1} = 1-r$
- $\frac{s_2-s_1}{s_3-s_1} = \frac{1}{1-r}$
- $\frac{s_2-s_3}{s_1-s_3} = \frac{r}{r-1}$
- $\frac{s_1-s_3}{s_2-s_3} = \frac{r-1}{r}$

Therefore addition Cayley graphs of ratio r, $\frac{1}{r}$, $1-r$, $\frac{1}{1-r}$, $\frac{r}{r-1}$, $\frac{r-1}{r}$ are all isomorphic to one another. Again, for the sake of convenience, we will call such a selection of ratios a *ratio-cluster*. Of course not every ratio-cluster has to contain six distinct elements, as some might appear double or triple.

This places the number of non-isomorphic addition Cayley graphs over G of order p, prime, somewhere between $\frac{p}{6}$ and $p-2$.

With this in mind we can return to the counterexamples given before. Figure 4.6 is an example with $p = 19 \equiv 3 \mod 4$ and $S = \{3, 5, 6\}$ and thus also with ratio $\frac{p-1}{2}$.

For reasons of degree all dashed edges in this example would have to be contained in a Hamiltonian circuit. But using all these edges makes it impossible to include the highlighted vertex into the circuit, making this graph non-Hamiltonian. The same argument holds for all $p \equiv 3 \mod 4$ if the ensuing addition Cayley graph has ratio $\frac{p-1}{2}$.

If we now insert $\frac{p-1}{2}$ into the above equations as r, we get:

- $r = \frac{p-1}{2}$
- $\frac{1}{r} = p-2$
- $1-r = \frac{p-1}{2} + 2$

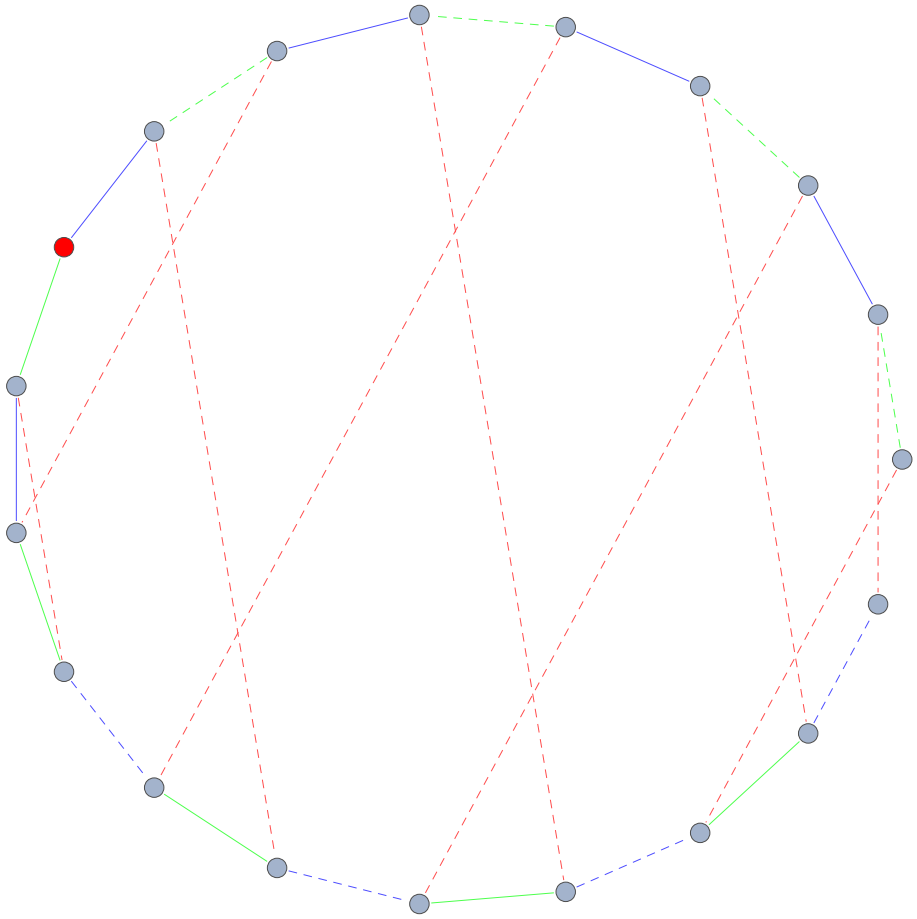


Figure 4.6: $Cay^{+}_{\mathbb{Z}_{19}}(\{3,5,6\})$ without self-loops; the 3-edges are blue, the 5-edges green and the 6-edges red; the highlighted vertex is the root of 6

- $\frac{1}{1-r} = \frac{2}{3}$
- $\frac{r}{r-1} = \frac{1}{3}$
- $\frac{r-1}{r} = 3$

and thus the following proposition:

Proposition 4.22. *Let G be a cyclic group of order p, where p is an odd prime with $p \equiv 3 \mod 4$, and $S = \{s_1, s_2, s_3\}$ a subset of G of cardinality 3.*

If $r\left(Cay^{+}_{G}(S)\right)$ is equal to one of the values:

- $\frac{p-1}{2}$

- $p-2$
- $\frac{p-1}{2}+2$
- $\frac{2}{3}$
- $\frac{1}{3}$
- 3,

then $Cay_G^+(S)$ is not Hamiltonian.
We will call this ratio-cluster the 3-cluster.

Naturally, the question arises whether this is the only ratio-cluster which causes $Cay_G^+(S)$ to be non-Hamiltonian. Using an exhaustive search, based on the above, for primes less than and including 79, the author came to the following results: For $p = 7, 11, 31, 67, 71, 79$ the only ratio-cluster leading to non-Hamiltonian graphs is the 3-cluster. For $p = 19, 23, 43, 47, 53$ we receive one more cluster each:

- $p = 19$: $\{8, 12\}$
- $p = 23$: $\{4, 6, 9, 15, 18, 20\}$
- $p = 43$: $\{7, 37\}$
- $p = 47$: $\{4, 12, 17, 31, 36, 44\}$
- $p = 53$: $\{4, 15, 21, 39, 45, 56\}$.

In the statement of Conjecture 4.13 in [CL] the cardinality of 4 for the subset S is motivated by the fact that there are counterexamples for this conjecture for S of cardinality 3. But the counterexamples we have seen so far are all over groups of order $|G| \equiv 3 \mod 4$, and in fact no other such examples are known.

This gives rise to the following conjecture:

Conjecture 4.23. *Let G be a finite cyclic such that $|G| \equiv 1 \mod 4$.*
Suppose $S \subseteq G$ with cardinality at least 3 such that $Cay_G^+(S)$ is connected, then $Cay_G^+(S)$ is Hamiltonian.

The author has verified this statement and Conjecture 4.18 for a few hundred instances over different groups of order less than 100 (as checking for Hamiltonicity is NP-complete) using random numbers as elements for S.

This can only be used as an argument if there is a small likelihood of isolated counterexamples which are unlikely to be reached using a random approach. But the structure of these graphs, as motivated by the preceding, seems to imply that the existence of one counterexample would lead to a large number of counterexamples through isomorphy.

For groups of prime order we have shown that there are very few different graphs, so that the following weaker statement can be justified much more effectively:

Conjecture 4.24. *Let G be a finite cyclic group with $|G| \equiv 1 \mod 4$ prime.*

Let S be a subset of G with cardinality at least 3 such that $Cay_G^+(S)$ is connected, then $Cay_G^+(S)$ is Hamiltonian.

This statement has been checked by the author using an exhaustive search (i.e. checking all instances) for primes up to and including 89.

What we have seen so far suggests a possible strategy for proving Conjecture 4.13:

The easiest statement to prove seems to be Conjecture 4.24, as these graphs have a strong structure. This information could then in turn be used to prove Conjecture 4.23, answering our question for all odd numbers $\equiv 1 \mod 4$.

For odd numbers $\equiv 3 \mod 4$ the statement is probably harder to show. One would have to find a structure in the ratio-clusters that are unequal to the 3-cluster and motivate why, in these cases, adding one element to S would lead to Hamiltonicity. If we have shown the statement for primes, it should then again be possible to expand this result to all other odd numbers.

Conclusion

In the course of this work, we have seen that addition Cayley graphs are not only interesting because of their simple and pleasing construction, but that these graphs also have relevance to other important fields of mathematics, such as additive combinatorics.

In the first part of this work, we have shown that addition Cayley graphs furnish us with a new tool to combine graph theory and additive combinatorics. Therefore, it seems pertinent to examine their properties closer.

In the last chapter, we have made some progress toward solving the problem of Hamiltonicity. We have shown the existence of Hamiltonian paths on addition Cayley graphs over cyclic groups of prime and prime-power cardinality. Further, we have made some progress toward a conjecture [CL] about Hamiltonicity of addition Cayley graphs on cyclic groups in general, by making observations on the structure of the special case of prime cardinality groups.

Also, we have given new conjectures (4.23 and 4.24) which strengthen Conjecture 4.13, but make a new prerequisite on the size of the underlying cyclic group.

While computations and heuristic arguments show that these conjectures are likely to hold, they are still far from being proven. However, this work has shown where Hamiltonicity does not hold for addition Cayley graphs over cyclic groups and sets S of cardinality 3, i.e. for specific sets S (see Proposition 4.22). Therefore, it would be a big step to show why adding another element to S makes addition Cayley graphs over these sets Hamiltonian.

To prove Conjecture 4.13 fully, it will also be necessary to inspect addition Cayley graphs over cyclic groups of even cardinality. In this context, it is possible to use the results from [CGW03] for square-free sets S. The other cases seem to be quite difficult, as one will need to make case-distinctions on the number of squares contained in S.

If the conjectures given in this work should be proved, it would be the logical step to examine addition Cayley graphs over other groups with small generating sets, for example of size two or three. As [Lev10] states that the size of S must be at least the rank of G, feasible results for groups with large generating sets are out of the question.

Not only the question of Hamiltonicity should be further clarified, many graph invariants, such as the chromatic number, are still completely unstudied. Other properties, such as the diameter, the independence number (see Section 3.3) and the clique number (see Section 3.2) have only been treated partially and still remain unclear.

The more discovered about these properties, the more the relationship to additive combinatorics can be exploited, to find new results or possibly simpler graph-theoretical proofs for old results.

Summing up, addition Cayley graphs offer a variety of open questions, and their structure make it likely that interesting results can be found.

Bibliography

[AABL09] N. Alon, O. Angel, I. Benjamini, and E. Lubetzky. Sums and products along sparse graphs. *Arxiv*, 2009.

[Alo86] N. Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):83 – 96, 1986.

[Alo07] N. Alon. Large sets in finite fields are sumsets. *Journal of Number Theory*, 126(1):110 – 118, 2007.

[AM85] N. Alon and V.D. Milman. λ_1, isoperimetric inequalities for graphs, and superconcentrators. *Journal of Combinatorial Theory, Series B*, 38(1):73 – 88, 1985.

[AR05] N. Alon and V. Rödl. Sharp bounds for some multicolor ramsey numbers. *Combinatorica*, 25:125–141, 2005.

[BG08] J. Bourgain and A. Gamburd. Uniform expansion bounds for cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. *Annals of Mathematics*, 167:625 – 642, 2008.

[BT04] J. Bourgain and T. Tao. A sum-product estimate in finite fields, and applications. *Geometric and Funktional Analysis*, 14(1):27 – 57, 2004.

[CGW03] B. Cheyne, V. Gupta, and C. Wheeler. Hamilton cycles in addition graphs. *Rose-Hulman Undergraduate Math. Journal*, 1(4), 2003.

[Chu89] F. R. K. Chung. Diameters and eigenvalues. *Journal of the American Mathematical Society*, 2(2):187–196, 1989.

[CL] E. Croot and V. F. Lev. Open problems in additive combinatorics.

[DGMS09] M. DeVos, L. Goddyn, B. Mohar, and R. Sámal. Cayley sum graphs and eigenvalues of (3,6)-fullerenes. *Journal of Combinatorial Theory, Series B*, 99(2):358 – 369, 2009.

[Dod84] J. Dodziuk. Difference equations, isoperimetric inequality and transience of certain random walks. *Transactions of the American Mathematical Society*, 284(2):787 – 794, 1984.

[Fre73] G.A. Freiman. *Foundations of a Structural Theory of Set Addition*, volume 37 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, R.I., 1973.

[Fri93] Joel Friedman. Some geometric aspects of graphs and their eigenfunctions. *Duke Mathematical Journal*, 69:487 – 525, 1993.

[Fro96] G. Frobenius. Über gruppencharaktere. *Sitzungsberichte der Köniqlich Preußischen Akademie der Wissenschaften zu Berlin*, page 985–1021, 1896.

[Gal68] T. Gallai. *On Directed Paths and Circuits, in "Theory of Graphs"*. Academic Press, New York, 1968.

[Gam02] A. Gamburd. Spectral gap for infinite index "congruence" subgroups of $SL_2(\mathbb{Z})$. *Israel Journal of Mathematics*, 127:157 – 200, 2002.

[GHS09] A. Gamburd, S. Hoory, and M. Shahshahani. On the girth of random cayley graphs. *Random Structures and Algorithms*, 35(1):100 – 117, 2009.

[GLS07] D. Grynkiewicz, V. F. Lev, and O. Serra. The connectivity of addition cayley graphs. *Electronic Notes in Discrete Mathematics*, 29:135 – 139, 2007.

[GM05] H. Glover and D. Marušič. Hamiltonicity of cubic cayley graphs. *Arxiv*, 2005.

[Gow01] W.T. Gowers. A new proof of szemerédi's theorem. *Geometric and Funktional Analysis*, 11(3):465 – 588, 2001.

[Gre05] B. Green. Counting sets with small sumset, and the clique number of random cayley graphs. *Combinatorica*, 25:307–326, 2005.

[GT08] B. Green and T. Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167(2):481 – 547, 2008.

[Hel08] H. Helfgott. Growth and generation in $SL_2(\mathbb{Z}\backslash p\mathbb{Z})$. *Annals of Mathematics*, 167(2):601 – 623, 2008.

[HLW06] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their application. *Bulletin of the American Mathematical Society*, 43:439 – 561, 2006.

[Kon03] S. Konyagin. A sum-product estimate in fields of prime order. *Arxiv*, 2003.

[Lev05] V.F. Lev. Restricted set addition in abelian groups: Results and conjectures. *Journal de Théorie des nombrés de Bordeaux*, 17:181 – 193, 2005.

[Lev10] Vsevolod F. Lev. Sums and differences along hamiltonian cycles. *Discrete Mathematics*, 310(3):575 – 584, 2010.

[Lov70] L. Lovász. *Combinatorial Structures and their Applications*. (Proc. Calgary Internat. Conf., Calgary, Alberta, 1969). Gordon and Breach, New York, 1970.

[Lub94] A. Lubotzky. *Discrete Groups, Expanding Graphs and Invariant Measures*, volume 125 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1994.

[Lub95] A. Lubotzky. Cayley graphs: Eigenvalues, expanders and random walks. In P. Rowbinson, editor, *Surveys in Combinatorics*, volume 18 of *London Mathematical Lecture Note Series*, pages 155 – 189. Cambridge University Press, Cambridge, 1995.

[Mar73] G. A. Margulis. Explicit constructions of expanders. *Problemy Peredači Informacii*, 9(4):71 – 80, 1973.

[Mar83] D. Marušič. Hamiltonian circuits in cayley graphs. *Discrete Mathematics*, 46(1):49 – 54, 1983.

[NA95] I.Z.Ruzsa N. Alon, M.B. Nathanson. Adding distinct congruence classes modulo a prime. *American Mathematical Monthly*, 102:250 – 255, 1995.

[NA96] I.Z.Ruzsa N. Alon, M.B. Nathanson. The polynomial method and restricted congruence classes. *Journal of Number Theory*, 56:404 – 417, 1996.

[Nil91] A. Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207 – 210, 1991.

[RS59] E. Rapaport-Strasser. Cayley color groups and hamilton lines. *Scripta Mathematica*, 24:51–58, 1959.

[San47] L. N. Sanov. A property of a representation of a free group. *Doklady Akademii Nauk SSSR*, 57:657 – 659, 1947.

[SX91] P. Sarnak and X. Xue. Bounds for multiplicities of automorphic representations. *Duke Mathematical Journal*, 64:207 – 227, 1991.

[Tao08] T. Tao. Product set estimates for non-commutative groups. *Combinatorica*, 28(5):547 – 594, 2008.

[TV06] T. Tao and V. Vu. *Additive Combinatorics*. Cambridge University Press, Cambridge, 2006.