Distinguishing Chromatic Number of Random Cayley graphs

Niranjan Balachandran* and Sajith Padinhatteeri †
Department of Mathematics
Indian Institute of Technology Bombay
Mumbai, India.

Abstract

The *distinguishing chromatic number* of a graph G, denoted $\chi_D(G)$, is defined as the minimum number of colors needed to properly color G such that no non-trivial automorphism of G fixes each color class of G. In this paper, we consider random Cayley graphs Γ defined over certain abelian groups A with $|A| = n$, and show that with probability at least $1 - n^{-\Omega(\log n)}$, $\chi_D(\Gamma) \leq \chi(\Gamma) + 1$.

Keywords: Distinguishing Chromatic Number, Random Cayley graphs.

2010 AMS Classification Code: 05C15, 05C25, 05C80.

1 Introduction

Let G be a graph and let $\mathrm{Aut}(G)$ denote its full automorphism group. Albertson and Collins introduced the notion of the *distinguishing number of a graph* in [2].

Definition 1. *A labeling of vertices of a graph $G, h : V(G) \to \{1, \ldots, r\}$ is said to be* **distinguishing** *(or r-distinguishing) provided no nontrivial automorphism of the graph preserves all of the vertex labels. The distinguishing number of a graph G, denoted by $D(G)$, is the minimum r such that G has an r-distinguishing labeling.*

Collins and Trenk introduced the notion of the distinguishing chromatic number in [7] as follows.

Definition 2. *A labeling of vertices of a graph $G, h : V(G) \to \{1, \ldots, r\}$ is said to be* **proper distinguishing** *(or proper r-distinguishing) provided the labeling is proper and distinguishing. The distinguishing chromatic number of a graph $G, \chi_D(G)$, is the minimum r such that G has a proper r-distinguishing labeling.*

*Supported by grant 12IRCCSG016, IRCC, IIT Bombay
†Supported by grant 09/087(0674)/2011-EMR-I, Council of Scientific & Industrial Research, India

In other words, the distinguishing chromatic number of a graph G is the smallest integer r such that the vertex set can be partitioned into sets $V_1, V_2, \ldots, V_r$ such that each V_i is independent in G, and for every $1 \neq \pi \in \mathrm{Aut}(G)$ there exists some color class V_i such that $\pi(V_i) \neq V_i$. While the presence of the graph in the definition of the distinguishing number is merely in order to invoke the group action, the graph itself has a more central (and combinatorially important) role in the notion of the distinguishing chromatic number. Since this notion is distinct from the notion of the chromatic number only when the graph admits non-trivial automorphisms, it is a matter of specific interest to determine the distinguishing chromatic number of graphs with a large automorphism group.

It must be remarked here that the distinguishing chromatic number of a graph G can behave quite haphazardly in contrast to the size of $\mathrm{Aut}(G)$ (see [4] for examples highlighting this aspect). However, there are results that establish a bound on $\chi_D(G) - \chi(G)$ in terms of its automorphism group. Indeed, a result of Collins, Hovey, and Trenk [6] states that if $\mathrm{Aut}(G) = \mathbb{Z}_{p_1^{i_1}} \times \mathbb{Z}_{p_2^{i_2}} \times \cdots \times \mathbb{Z}_{p_k^{i_k}}$ (in particular, $\mathrm{Aut}(G)$ is abelian), then $\chi_D(G) \leq \chi(G) + k$, so for instance, if $\mathrm{Aut}(G)$ is a cyclic group of prime power order, then $\chi_D(G) \leq \chi(G) + 1$. A more relevant result (in our context) of Seress [11] states that if G is a vertex transitive graph with a solvable automorphism group, then $\chi_D(G) \leq \chi(G) + 4$. Thus, while one cannot correlate this gap with the size of the automorphism group of G, there is reason to believe that *in most cases*, it is heuristically a valid perspective that a graph that has a 'small automorphism group' must have a small gap $\chi_D(G) - \chi(G)$.

Note that an 'average' graph, i.e., an Erdős-Renyi random graph $G(n,p)$ is very likely a rigid graph, i.e., it has no non-trivial automorphisms. Thus, to make this question less trivial, one needs to consider a typical graph arising from a family of graphs that admit non-trivial automorphism groups, and one class of graphs that do so are Cayley graphs of groups. To recall the definition, let A be a finite group with cardinality n and let $S \subset A$ with $1 \notin S$ be an inverse closed subset of A. In other words, $S = S^{-1}$ where $S^{-1} := \{g^{-1} : g \in S\}$. The Cayley graph of A with respect to S, denoted by $\Gamma(A,S)$ is the following graph: $V(\Gamma(A,S)) = A$ and $E(\Gamma(A,S)) = \{(g,gh) : g \in A, h \in S\}$. It is straightforward to see that the group A acts regularly on $\Gamma(A,S)$. If A is abelian, the map $i(g) = g^{-1}$ is also an automorphism of A which is distinct from any of the automorphisms induced by the member of A unless $A \simeq \mathbb{F}_2^r$ for some $r \in \mathbb{N}$. Hence, for A abelian, it is easy to see that $A \rtimes \langle i \rangle \subseteq \mathrm{Aut}(\Gamma(A,S))$. If equality holds here, then we say that $\Gamma(A,S)$ has automorphism group *as small as possible*.

A conjecture of Babai and Godsil (see [3]) states that if A is an abelian group of order n, the proportion of inverse closed subsets S for which the corresponding Cayley graph $\Gamma(A,S)$ has automorphism group as small as possible tends to 1, as $n \to \infty$. This conjecture was proved in [3] for abelian groups with $n \equiv 3 \pmod 4$. In a recent paper by Dobson, Spiga and Veret [8], this conjecture has been settled in the affirmative for all n.

In this paper, we restrict our attention to random Cayley graphs over certain kinds of abelian groups, with the group operation expressed additively. The model for the random graphs on Cayley groups that we shall consider is described as follows. Let A be a finite group with $|A| = n$, and let $0 < p = p(n) < 1$. Each element $g \in A$ of order 2 is chosen with probability p and for any other $x \in A$, the pair $(x, -x)$ is chosen with probability p and all these random choices are made independently to form the set S. The random Cayley graph is the graph $\Gamma_p := \Gamma(A,S)$. Thus, the

main theorem of [8] may be written as

$$\mathbb{P}\Big(A \rtimes \langle i \rangle \subsetneq \mathrm{Aut}(\Gamma_{1/2}(A,S))\Big) \to 1 \text{ as } n \to \infty.$$

In order to state our results, we first set up some notation. We write $f(n) = O(g(n))$ if there exists a constant $K > 0$ such that $|f(n)| \leq K|g(n)|$ for all n and write $f(n) = \Omega(g(n))$ if there exists a constant $c > 0$ such that $|f(n)| \geq c|g(n)|$ for all n. Finally, we write $f(n) \ll g(n)$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$. By log we shall mean $\log_2$ throughout the paper.

Usually, the phrase 'E_n occurs with high probability' refers to the statement, $\mathbb{P}(E_n) \to 1$ as $n \to \infty$ for some relevant parameter n. We shall in fact state a more precise rate of convergence, so our usage of the same phrase shall mean that $\mathbb{P}(E_n) \geq 1 - \Omega(n^{-\log n})$ for sufficiently large n, so that in particular, if an event E_n holds *whp*, then it holds with probability at least $1 - 1/n^c$ for any positive constant c. In all our statements, $n = |A|$, the size of the underlying group.

The first result we prove - which may be of independent interest - generalizes the result in [8] stated above, for a much larger range of p.

Theorem 3. *Let $\Gamma_p := \Gamma_p(A,S)$ be the random Cayley graph with $\frac{25(\log n)^2}{n} \leq p \leq 1 - \frac{25(\log n)^2}{n}$. Then,*

$$\mathbb{P}(\mathrm{Aut}(\Gamma_p) \ncong A \rtimes \langle i \rangle) \leq O(\exp(-\log^2 n)),$$

where $i : A \to A$ is the automorphism $i(x) = -x$. In particular, whp $\mathrm{Aut}(\Gamma_p)$ is as small as possible.

The focal point of this paper is to consider the distinguishing chromatic number for random Cayley graphs, and show that the heuristic expressed earlier is valid, i.e.,

$$\chi_D(\Gamma) \leq \chi(\Gamma) + 1 \textit{ with high probability (whp).}$$

However, in this paper, we restrict our focus to random Cayley graphs on groups of the following types:

1. The random Cayley graph $\Gamma_p(A,S)$, with $(|A|, 6) = 1$.
2. The random Cayley graph $\Gamma_p(A,S)$, where $A \cong \mathbb{Z}_2^r \times N$, and N is an odd order group which is not cyclic.

We shall call these as abelian groups of Type I and Type II respectively. Type I groups also appear in [9] where the chromatic number of a random Cayley graph $\Gamma_{1/2}(A,S)$ is determined asymptotically, though the Cayley graphs in [9] are sum Cayley graphs, i.e., x, y are adjacent in Γ if and only if $x + y \in S$, and S is picked uniformly at random from A.

The principal reason for restricting our attention to these families is that the results we obtain are much nicer to state in these cases. Some of the specific restrictions on A that appear for Type

II groups in our results may be relaxed, but our methods make the corresponding results a lot messier to state, so we restrict our attention to these families only.

Our main results in this paper are

Theorem 4 (**Distinguishing Chromatic Number for Random Cayley graphs on Type I groups**). *Let $\Gamma_p := \Gamma_p(A, S)$ be the random Cayley graph with*

$$\frac{25(\log n)^2}{n} \leq p \leq 1 - 19\left(\frac{\log n}{n}\right)^{2/3},$$

where A is an abelian group with order co-prime to six. Then,

$$\mathbb{P}\Big(\chi_D(\Gamma) \leq \chi(\Gamma) + 1\Big) \geq 1 - n^{-\Omega(\log n)}.$$

In particular, $\chi_D(\Gamma_p) \leq \chi(\Gamma) + 1$ with high probability.

and

Theorem 5 (**Distinguishing Chromatic Number for Random Cayley graphs on Type II groups**). *Suppose $A \cong \mathbb{Z}_2^r \times N$, where N is an odd order group which is not cyclic, $|A| = n$ and suppose that $m \ll \frac{n}{\log^2 n}$. Let $\Gamma_p := \Gamma_p(A, S)$ be the random Cayley graph with*

$$\frac{25(\log n)^2}{n} \leq p \leq \frac{7}{13(m + 2\log 2n)}.$$

Then

$$\mathbb{P}\Big(\chi_D(\Gamma_p) \leq \chi(\Gamma_p) + 1\Big) \geq 1 - n^{-\Omega(\log n)}.$$

In particular, $\chi_D(\Gamma_p) \leq \chi(\Gamma) + 1$ with high probability.

Note that the range for p in either case is quite varied. For groups of Type I, our results hold for a much larger range for p, whereas for groups of Type II, the range of p that we consider in our results only allows for sparse graphs on these groups. Again, this is owing to the ideas involved in the proofs for either case.

The rest of the paper is organized as follows. In the next section, we begin with some preliminaries, while also recalling the main results of [8] and their relevance to our work here. In Section 3, we prove Theorem 3. In Section 4 we prove Theorem 4 for random Cayley graphs on abelian groups of Type I, and in section 5, we prove Theorem 5 for random Cayley graphs on abelian groups of Type II. Finally, we close with some concluding remarks, some questions, and a conjecture. We make no attempt to obtain optimal constants in our results.

2 Preliminaries

In what follows, we borrow our notation and terminology from [8] which we restate for convenience of the reader.

Definition 6. *Let A be an abelian group and let $1 < H \leq K \leq A$ be subgroups of A. We say that the Cayley graph $\Gamma(A, S)$ is a generalized wreath graph with respect to (H, K, A) if $S \setminus K$ is a union of H-cosets.*

Definition 7. *The direct product of two graphs $G(V_1, E_1)$, $H(V_2, E_2)$ is the graph with vertex set $V_1 \times V_2$ and $e = (u_1, v_1)(u_2, v_2)$ is an edge if and only if $u_1u_2 \in E_1$ and $v_1v_2 \in E_2$.*

We need one further definition, namely, that of a *generalized dihedral group*.

Definition 8. *For an abelian group H, the generalized dihedral group of H is the semidirect product of H and Z_2, with Z_2 acting on H by inverting elements.*

One of the main theorems proved in [8] is the following.

Theorem 9. *Let G be a permutation group with an abelian regular subgroup A and a proper subgroup B which is generalized dihedral on A and such that $N_G(A) = B$. Then one of the following occurs:*

1. *$|A|$ is not a prime power and there exist two groups H an K with $1 < H \leq K < A$, and for every graph Γ with $G \leq \mathrm{Aut}(\Gamma)$, we have that Γ is a generalized wreath graph with respect to (H, K, A),*

or

2. *there exist two groups C and Z with $A = C \times Z$, with $C \cong C_t$ for some $t \geq 4$ and with Z an elementary abelian 2-group, such that, for every graph Γ with $G \leq \mathrm{Aut}(\Gamma)$, we have that Γ is isomorphic to the direct product of Λ with a Cayley graph over Z, where Λ is either complete or edgeless, possibly with loop at each vertex.*

The proof of Theorem 3 will follow from lemmas 12, 11, and 14 (see section 3 for their precise statements). Briefly speaking, Lemma 11 states that *whp* the normalizer of A in $\mathrm{Aut}(\Gamma_p)$ is $A \rtimes \langle i \rangle$. Lemma 12 and Lemma 14 state that *whp*, neither event as outlined as the two possible cases in Theorem 9 occurs, so Theorem 3 follows from Theorem 9.

The proofs of Theorems 4 and 5 use the structure of the automorphism group, and its size, respectively, along with a few additional ideas. We shall outline their proofs in the respective sections.

3 Proof of Theorem 3

In this section, we show that the results of [8] may be extended to the model of random graphs we are interested in, using very similar ideas, but for a much wider range of $p(n)$. We shall implicitly assume that n is sufficiently large whenever the need arises.

The number of elements of the group A whose order is at most two, is denoted by m.

Lemma 10. *Suppose $n \geq 2^{48}$. If $\frac{3}{2} \leq c_1, c_2 \leq n$ satisfy $c_1 c_2 \geq \frac{n}{24}$, and $p \in [\frac{25(\log n)^2}{n}, 1 - \frac{25(\log n)^2}{n}]$, then*

$$n^{\log n}(p^{c_1} + (1-p)^{c_1})^{c_2} < 3n^{-(\log n)/24}.$$

Proof. Consider $f(p) = (p^{c_1} + (1-p)^{c_1})^{c_2}$ on the interval $[0,1]$. It follows (by standard calculus) that $f(p)$ attains minimum at $p = \frac{1}{2}$. In particular, for $p \in [\frac{25(\log n)^2}{n}, 1 - \frac{25(\log n)^2}{n}]$, $f(p)$ attains its maximum value at the endpoints. Therefore, it suffices to prove the statement when $p = \frac{25(\log n)^2}{n}$ since f is symmetric about $1/2$.

Now,

$$(p^{c_1} + (1-p)^{c_1})^{c_2} \leq e^{-pc_1c_2}\, e^{c_2 y^{c_1}}$$

where $y = \frac{p}{1-p}$.

For $p \in [\frac{25(\log n)^2}{n}, 1/2]$, observe that

$$c_2 y^{c_1} \leq c_2 \left(\frac{25(\log n)^2}{n - 25(\log n)^2} \right)^{c_1} \leq n \left(\frac{25(\log n)^2}{n - 25(\log n)^2} \right)^{2/3} \leq 1. \tag{1}$$

The last inequality follows from the assumptions that $c_1 \geq 3/2$, $c_2 \leq n$, and the fact that $n \geq 2^{48}$. Therefore

$$n^{\log n}(p^{c_1} + (1-p)^{c_1})^{c_2} \leq e^{(\log n)^2 - pc_1c_2 + 1}.$$

Since $c_1 c_2 \geq n/24$ the right hand side in the last inequality is at most $\exp(-\frac{\log^2 n}{24} + 1)$. This completes the proof. □

For $S \subset A$ and $\phi \in \mathrm{Aut}(A)$, we say that ϕ *normalizes* S if $\phi(S) = S$. In what follows, unless otherwise mentioned, $p \in [\frac{25(\log n)^2}{n}, 1 - \frac{25(\log n)^2}{n}]$.

Lemma 11. *Suppose A is abelian, and let S be a random inverse closed subset of A with each pair $(x, -x)$ picked with probability p. Let $i : A \to A$ be the automorphism of A defined by $i : x \to -x$. Then the probability that there exists $\phi \in \mathrm{Aut}(A) \setminus \{1, i\}$ such that S is normalized by ϕ is at most $O(\exp(-\frac{21}{4}(\log n)^2)$. In particular, whp the normalizer of A in $\mathrm{Aut}(\Gamma_p)$ is $A \rtimes \langle i \rangle$.*

Proof. Fix $\phi \in \mathrm{Aut}(A)$ and suppose that ϕ normalizes S. Since $|i| = 2$, we have $m = |C_A(i)|$ where $C_A(i)$ is the centralizer of i in A. Let $|C_A(\phi)| = c$ and $|C_A(\langle i, \phi \rangle)| = k$.
Suppose that $|\phi|$ is divisible by an odd prime q.
In this case, without loss of generality we assume $|\phi| = q$, otherwise we may replace ϕ with a suitable power. Observe that, if $a \in S$ then $\{a, \phi(a), \ldots, \phi^{q-1}(a)\} \subseteq S$. Therefore,

$$\mathbb{P}\big(\phi(S) \subset S\big) = (p^q + (1-p)^q)^{\frac{m-k}{q}} (p^q + (1-p)^q)^{\frac{n-(c+m-k)}{2q}} \leq (p^q + (1-p)^q)^{\frac{n}{4q}}.$$

The last inequality follows by using $k \leq m, c \leq \frac{n}{2}$ and $(p^q + (1-p)^q) \leq 1$. Observe that an automorphism is completely determined once it is known on a set of generators of a group. For a group G with $|G| = n \geq 2$, there is a set $\mathfrak{G}$ of at most $\lfloor \log n \rfloor$ generators. Since there are at most

$n^{|\mathfrak{G}|}$ choices of maps on G, it follows that $|\mathrm{Aut}(G)| \leq n^{\log n}$. Therefore, the probability that there exists $\phi \in \mathrm{Aut}(A) \setminus \{1, i\}$ such that $\phi(S) = S$ is at most $n^{\log n}(p^q + (1-p)^q)^{\frac{n}{4q}}$. Using lemma 10, by setting $c_1 = q$ and $c_2 = \frac{n}{4q}$, we see that this probability is $O(\exp(-\frac{21}{4}(\log n)^2)$.

Now suppose $|\phi|$ is a power of two. Two cases arise:
Case 1: $i \in \langle\phi\rangle$
By replacing ϕ by a suitable power, we may assume that $\phi^2 = i$. Then,

$$\mathbb{P}(\phi(S) \subset S) = (p^2 + (1-p)^2)^{\frac{m-c}{2}}(p^2 + (1-p)^2)^{\frac{n-m}{4}} \leq (p^2 + (1-p)^2)^{\frac{n}{8}}.$$

The last inequality is obtained by using $m \leq \frac{n}{2}$ and $c \leq m$. Again, we use lemma 10 with $c_1 = 2$ and $c_2 = \frac{n}{8}$ to see that the above probability is at most $2^{(\log n)^2}(p^2 + (1-p)^2)^{\frac{n}{8}} \leq O(\exp(-\frac{21}{4}(\log n)^2)$.

Case 2: $i \notin \langle\phi\rangle$
In this case

$$\mathbb{P}(\phi(S) \subset S) = (p^2 + (1-p)^2)^{\frac{m}{2}}(p^2 + (1-p)^2)^{\frac{n-m}{4}} = (p^2 + (1-p)^2)^{\frac{m+n}{4}}.$$

Again, setting $c_1 = 2, c_2 = \frac{m+n}{4}$ and applying lemma 10 we see that the above probability is at most $O(\exp(-\frac{23}{2}(\log n)^2)$.

Finally, writing $\mathcal{G} = \mathrm{Aut}(\Gamma_p(A, S))$, note that if the normalizer of A in $\mathcal{G}$ strictly contains $A \rtimes \langle i\rangle$ then there exists $\phi \in N_{\mathcal{G}}(A) \setminus (A \rtimes \langle i\rangle)$ such that $\phi(S) = S$, but the probability that this occurs is bounded above by the expression of the lemma. □

Lemma 12. *Suppose A is an abelian group which is not a 2-group, and suppose S is chosen randomly by picking each pair*[1] *$(x, -x)$ independently with probability p where $\frac{25(\log n)^2}{n} \leq p \leq \frac{1}{2}$. Then,*

$$\mathbb{P}(\textit{There exist } 1 < H \leq K < A) \textit{ such that } S \setminus K \textit{is a union of } H - \textit{cosets}) \leq O(\exp(-\log^2 n)).$$

Proof. Observe that since $H \subset K \subset A$, $A \setminus K$ is also a union of H- cosets, and let the set of these cosets be denoted $\mathcal{H}$. Write $A' := A \setminus K$ and $S' := S \setminus K$. We shall denote the order of an element a by $o(a)$ and $a + a$ is denoted $2a$.

Define

$$\begin{aligned} M &:= \{a \in A : o(a) \leq 2\}, \\ J &:= K \cap M, \\ I &:= \{a \in A' : 2a \in H\}, \\ I' &:= A \setminus (K \cup I), \\ L &:= \{a \in H : o(a) = 2\}. \end{aligned}$$

Let $|H| = h$, $|I| = i$, $|K| = k$, $|J| = j$ and $|L| = l$. We have $|M| = m$.

[1] If $x = -x$ then the pair is just the singleton $\{x\}$

Fix subgroups $H < K$. To calculate $\mathbb{P}(S \setminus K$ is a union of $H-$cosets) first observe that if S' is a union of H-cosets, then,

$$g \in S' \Rightarrow g + H \subseteq S'.$$

In other words, for a fixed $g \in A'$, either $g + H \subseteq S'$ or $g + H$ and S' are disjoint. Hence the probability that S' is a union of H-cosets is precisely

$$\mathbb{P}\left(\bigcap_{g+H \in \mathcal{H}} \left\{(g + H \subseteq S) \text{ or } (g + H \cap S = \emptyset)\right\}\right). \tag{2}$$

Since A' is the disjoint union of I and I', we consider the two cases $g \in I'$ and $g \in I$ to calculate the expression in (2).

$g \in I'$: Suppose $h_1 \in H$, and if possible let $g + h_1 \in K \cup I$. If $g + h_1 \in K$ then we have $g \in K$ since $H \subseteq K$. But this contradicts the assumption $g \in I'$. If $g + h_1 \in I$ then by the definition of I, we have $2g + 2h_1 = h_2$ for some $h_2 \in H$. Therefore $2g \in H$ and $g \in I$ which contradicts the assumption on g. Consequently, if $g \in I'$ then $g + H \subseteq I'$.

We further note that if $g \in I'$ then $-g \notin g + H$, otherwise we have $-g = g + h$ for some $h \in H$ and hence $2g \in H$ which contradicts the assumption that $g \in I'$. Also, observe that $I' \cap M = \emptyset$ because $g \in I' \cap M$ and $o(g) \leq 2$ implies $2g = 0 \in H$ and $g \in I$. The upshot of the above discussion is the following: If $g \in I'$ then $g + H$ and $-g + H$ are two distinct cosets and are both contained in I'. Since each pair $(g, -g)$ is independently picked with probability p into S we have that

$$g + H \subseteq S' \iff -g + H \subseteq S'.$$

Since there are $\frac{n-k-i}{2h}$ pairs of cosets in I' of the type $(g + H, -g + H)$, the probability that for every $g + H \in I'$ either $g + H \subset S$ or $g + H \cap S = \emptyset$ is exactly $(p^h + (1-p)^h)^{\frac{n-k-i}{2h}}$.

$g \in I$: In this case note that $g + H = -g + H$. We consider the two sub-cases $o(g) \leq 2$ and $o(g) > 2$.

Suppose $o(g) \leq 2$. Then for $h \in H$, we have $2(g + h) = 0$ if and only if $o(h) = 2$. In particular, the number of order 2 elements in $g + H$ is precisely the number of order two elements in H. Since there are l elements in $g + H$ of order two and $h - l$ elements of order greater than two, and since the number of H cosets $g+H$ with $g \in I, o(g) = 2$ that contain order two elements is precisely $\frac{m-j}{l}$, the probability that every coset $g + H$ with $g \in M \cap I$ satisfies that $g + H \cap S = \emptyset$ or $g + H \subset S$ is precisely $(p^{\frac{h+l}{2}} + (1-p)^{\frac{h+l}{2}})^{\frac{m-j}{l}}$.

If $o(g) > 2$, then it follows that $g+H$ has no element of order two. There are exactly $i - \frac{m-j}{l}h$ elements $g \in I$ of this type and furthermore, the set of these elements must also necessarily be the union of $\frac{1}{h}(i - \frac{m-j}{l}h)$ H-cosets. If $g + H \subseteq S'$, one need to include the $\frac{h}{2}$ pairs $(x, -x)$ of the coset into S, so the probability that every $g + H$ with $o(g) > 2$ is either disjoint with S or is contained in S is precisely $(p^{\frac{h}{2}} + (1-p)^{\frac{h}{2}})^{(\frac{i}{h} - \frac{m-j}{l})}$.

Set $y := \frac{p}{1-p}$. Then, from the above discussions, for a fixed $H \subset K$, we have,

$$\begin{aligned}\mathbb{P}(S' = \text{ union of } H\text{- cosets}) &= (p^h + (1-p)^h)^{\frac{n-k-i}{2h}}(p^{\frac{h+l}{2}} + (1-p)^{\frac{h+l}{2}})^{\frac{m-j}{l}}(p^{\frac{h}{2}} + (1-p)^{\frac{h}{2}})^{(\frac{i}{h} - \frac{m-j}{l})} \\ &\leq (1-p)^{\frac{n}{4}} \exp(\frac{n-k-i}{2h} y^h) \exp(\frac{m-j}{l} y^{\frac{h+l}{2}}) \exp((\frac{i}{h} - \frac{m-j}{l}) y^{\frac{h}{2}})\end{aligned}$$

The last inequality is obtained by using the facts that $k \leq \frac{n}{2}$, $j \leq m$ and $(1-p) < 1$. Furthermore, note that we may without loss of generality assume that $p \in [\frac{25(\log n)^2}{n}, \frac{1}{2}]$. We shall now show that each of $\exp(\frac{n-k-i}{2h} y^h), \exp(\frac{m-j}{l} y^{\frac{h+l}{2}}), \exp((\frac{i}{h} - \frac{m-j}{l}) y^{\frac{h}{2}})$ is bounded.

If $h > 2$, then, using inequality (1) of lemma 10 and taking $c_1 = h, c_2 = \frac{n-k-i}{2h}$, it follows that $\exp(\frac{n-k-i}{2h} y^h)$ is bounded. Again using the same inequality, and taking $c_1 = \frac{h+l}{2} > 1$ and $c_2 = \frac{m-j}{l} \leq n$ it follows that $\exp(\frac{m-j}{l} y^{\frac{h+l}{2}})$ is bounded. As for $\exp((\frac{i}{h} - \frac{m-j}{l}) y^{\frac{h}{2}})$, we set $c_1 = \frac{h}{2} > 1$ and $c_2 = (\frac{i}{h} - \frac{m-j}{l}) < n$. To pick a pair of non-trivial subgroups H and K, it suffices to only pick sets of generators for these groups which can be done in at most $(n^{\log n})^2 = 2^{2\log^2 n}$ ways. Hence

$$\mathbb{P}(\text{There exist } 1 < H \leq K < A : |H| > 2, S \setminus K = \text{ union of } H - \text{cosets}) \leq O\left(2^{2(\log n)^2}(1-p)^{\frac{n}{4}}\right).$$

By lemma 10, we have $2^{2(\log n)^2}(1-p)^{\frac{n}{4}} \leq \exp(-\frac{17}{4}(\log n)^2)$ for $p \in [\frac{25(\log n)^2}{n}, \frac{1}{2}]$.

If $h = 2$, then, firstly note that if g satisfies $2g \in H$ then $o(g)|4$, so g lies in the Sylow 2-subgroup of A. Since A is not a 2-group by assumption, it follows that $i \leq n/3$. Hence using that $j \leq m, k \leq \frac{n}{2}$ we have

$$\begin{aligned}\mathbb{P}(S \setminus K \text{ is a union of} H - \text{cosets}) &= (p^2 + (1-p)^2)^{\frac{n-k-i}{4}}(p^{\frac{2+l}{2}} + (1-p)^{\frac{2+l}{2}})^{\frac{m-j}{l}} \\ &\leq (1-p)^{\frac{n}{12}} \exp(\frac{n-k-i}{4} y^2) \exp(\frac{m-j}{l} y^{\frac{2+l}{2}}) \qquad (3)\end{aligned}$$

As before, the boundedness of $\exp(\frac{n-k-i}{4} y^2)$ follows by setting $c_1 = 2$ and $c_2 = \frac{n-k-i}{4} < n$ and the boundedness of $\exp(\frac{m-j}{l} y^{\frac{2+l}{2}})$ follows by setting $c_1 = \frac{2+l}{2} > 1, c_2 = \frac{m-j}{l} < n$. Again,

$$\mathbb{P}(\text{There exist } 1 < H \leq K < A : |H| = 2, S \setminus K = \text{ union of } H - \text{cosets}) \leq O\left(2^{2(\log n)^2}(1-p)^{\frac{n}{12}}\right)$$

and by lemma 10, this is at most $\exp(-\frac{1}{4}(\log n)^2)$. □

Definition 13. *Let A be an abelian group of Type I or Type II. Let C be a cyclic group, and Z an elementary abelian 2 group. For a subset $S \subset A$, we call a pair of subgroups (C, Z) of A, good for S, if*

1. *$A = C \times Z$.*
2. *$|C| = t \geq 4$.*
3. *There exist $S' \in \{C, \emptyset, \{0\}, C \setminus \{0\}\}$, and $S'' \subset Z$ such that $S = S' \times S''$.*

Lemma 14. *For a random inverse-closed subset $S \subset A$, the probability that there exists a pair (C, Z) good for S is at most $O\left(\exp(-\frac{25(\log n)^2(n-1)}{2n})\right)$.*

Proof. If A is a group of type II, then the lemma is trivial as a simple consequence of the fundamental theorem of abelian groups. So, suppose A is a group of Type I and consider the Cayley graphs $\Gamma(A, S)$. If A satisfies the hypothesis of the lemma, then Z is necessarily trivial, and the lemma needs a proof only in the case where A is a cyclic group of order at least 4. This gives exactly four possible choices for $S' \in \{\emptyset, A, (0), A \setminus \{0\}\}$, and two possible choices for $S'' \in \{\emptyset, (0)\}$. However, since S is inverse-closed in A and $0 \notin S$, there are effectively only two possibilities for $S = S' \times S$", namely, $S = \emptyset$ and $S = A \setminus \{0\}$. If $S = \emptyset$ then the probability that there exist (C, Z, S', S'') satisfying the hypotheses mentioned above equals $(1-p)^{\frac{n+m-2}{2}} \leq O\left(\exp(-\frac{25(\log n)^2(n-1)}{2n})\right)$. Similarly, if $S = A \setminus \{0\}$ the corresponding probability equals $p^{\frac{n+m-2}{2}} \leq O\left(\exp(-\frac{25(\log n)^2(n-1)}{2n})\right)$. This completes the proof of the lemma.

□

We are now in a position to prove Theorem 3.

Proof of Theorem 3. Let $\mathcal{G} = \mathrm{Aut}(\Gamma_p)$ and let $B := A \rtimes \langle i \rangle$. Then B is generalized dihedral, A is an abelian regular subgroup of $\mathcal{G}$, and is normal in B, so $B \subseteq N_{\mathcal{G}}(A)$. By Lemma 11 and the observation that an automorphism ϕ of A is a graph automorphism if and only if $\phi(S) = S$, we have $N_{\mathcal{G}}(A) = B$ *whp.*

Now we prove $\mathcal{G} = B$ *whp.* First recall that B is generalized dihedral over A. In order to do that, consider the following events:

1. $\mathcal{E}_1$: There exist subgroups $H < K < A$ such that Γ_p is a generalized wreath graph with respect to (H, K, A).
2. $\mathcal{E}_2$: There exists a cyclic group C, and an elementary 2-group Z such that Γ_p is isomorphic to the direct product of Λ with a Cayley graph over Z, where Λ is either complete or edgeless, possibly with loop at each vertex.

If B is a proper subgroup of $\mathcal{G}$ then by Theorem 9 either $\mathcal{E}_1$ or $\mathcal{E}_2$ occurs, so $\mathbb{P}(B \neq \mathcal{G}) \leq \mathbb{P}(\mathcal{E}_1) + \mathbb{P}(\mathcal{E}_2)$. By Lemma 12, $\mathbb{P}(\mathcal{E}_1) \leq O(\exp(-\log^2 n))$. Note that $\mathcal{E}_2$ occurs only if A is a cyclic group of type I, and with $Z = \{0\}$ and $A \equiv C$, so If Γ_p is a direct product as described in $\mathcal{E}_2$, then $S = S' \times S$" with $S' \in \{\emptyset, C, C \setminus \{0\}, \{0\}\}$ and S" $= \{0\}$. But then by lemma 14,$\mathbb{P}(\mathcal{E}_2) \leq O(\exp(-\log^2 n))$, and this completes the proof. □

4 Random Cayley Graphs on Type I Groups: Proof of Theorem 4

Proof of Theorem 4. Recall that a type I group satisfies $(|A|, 6) = 1$. Set $|A| = n$.

We first give an outline of the proof. We show that *whp* there exists distinct non-zero $x, y, z \in A$ such that $x + y + z = 0$, and such that $\{x, y, z\}$ is independent in $\Gamma_p(A, S)$ *whp*. We shall see that these constraints on T imply that the only automorphism $\phi \in A \rtimes \langle i \rangle$ of the graph Γ_p that fixes T as a set is the trivial automorphism. Then, by giving a new color to these vertices and coloring the other vertices as frugally as possible, using at most $\chi(\Gamma_p(A, S))$ colors, it follows, in conjunction with Theorem 3, that $\chi_D(\Gamma_p) \leq \chi(\Gamma_p) + 1$ *whp*.

Our main probabilistic tool here is Janson's inequality which we state here for convenience.

Suppose $\mathcal{X}$ is a finite set, and let R be a random subset of $\mathcal{X}$ where each $r \in \mathcal{X}$ is chosen into R independently with probability p_r. Let $X_i \subset \mathcal{X}$ for $i = 1, 2 \ldots, t$, and let B_i denote the event: $X_i \subset R$. Let

$$N = \#\{i : X_i \subset R\}, \quad \mu := \mathbb{E}(N), \quad \Delta := \sum_{i \sim j} \mathbb{P}(B_i \wedge B_j),$$

where $i \sim j$ if $X_i \cap X_j \neq \emptyset$. Then Janson's inequality states that if $\mu \leq \Delta$ then

$$\mathbb{P}(N = 0) \leq \exp\left(-\frac{\mu^2}{2\Delta}\right)$$

The random process of picking S is equivalent to rejecting each pair $(x, -x)$ in A (for $x \neq 0$) independently with probability $q = 1 - p$.

Let $\mathcal{T} := \{\{x, y, z\} \subset A : x + y + z = 0, x \neq 0, y \neq 0, z \neq 0\}$ and for each $T \in \mathcal{T}$, let

$$D(T) := \{\pm(x - y), \pm(y - z), \pm(x - z)\}.$$

First, observe that $|\mathcal{T}| = \frac{(n-5)(n-1)}{6}$. Indeed, there are $n - 1$ choices for x with $x \neq 0$, and since $y \notin \{0, x, -x, 2x\}, 2y \neq -x$, there are $n-5$ choices for y and z is consequently determined uniquely, so that gives $(n - 1)(n - 5)$ ordered triples (x, y, z) satisfying the conditions of the sets in $\mathcal{T}$.

Consider the events B_T: $D(T) \subset \overline{S}$, and let $N = \#\{T \in \mathcal{T} : D(T) \subset \overline{S}\}$. Then

$$\mathbb{E}(N) = |\mathcal{T}|q^3 = \frac{(n - 5)(n - 1)}{6} q^3.$$

Observe that, $T \sim U$ if and only if $|D_T \cap D_U| \neq 0$ since otherwise the choices for the sets $T, U \in \mathcal{T}$ are decided over disjoint sets of inverse-closed pairs. Set

$$\Delta = \sum_{D(T) \cap D(U) \neq \emptyset} \mathbb{P}(B_T \wedge B_U)$$

We note by a straightforward calculation (see the Appendix for the details) that

$$\Delta < 3n|\mathcal{T}|q^5 + 6|\mathcal{T}|q^4 + 2|\mathcal{T}|q^3, \tag{4}$$

so by Janson's inequality, it follows that for $q \geq 19\left(\frac{\log n}{n}\right)^{2/3}$ we have

$$\mathbb{P}(N = 0) < \exp\left(\frac{-|\mathcal{T}|q^3}{2(3nq^2 + 6q + 2)}\right) = e^{-\Omega(\log^2 n)}.$$

Suppose $\sigma \in A \rtimes \langle i \rangle$ is non-trivial and $\sigma(T) = T$ for some $T \in \mathcal{T}$. If $\sigma = (g, 1)$ for some $g \in A$, and if $\sigma(x) = y, \sigma(y) = z, \sigma(z) = x$, say, then by the action of $(g, 1)$ on A, it follows that $3g = 0$ contradicting that σ is non-trivial. If $\sigma(x) = y, \sigma(y) = x$ and $\sigma(z) = z$, say, Then, it similarly follows that $2g = 0$, contradicting that σ is non-trivial. If $\sigma = (g, i)$ for some $g \in A$, and if $\sigma(x) = y, \sigma(y) = z$ and $\sigma(z) = x$, then since $(g, i)(x) = g - x$, it follows that $x = y = z$ contradicting that $\{x, y, z\} \in \mathcal{T}$. Again, if $\sigma(x) = y, \sigma(y) = x$ and $\sigma(z) = z$. Then, it follows that $2z - x = y$ and since $x + y + z = 0$, we have $2z = 0$, again, a contradiction to the assumption that $\{x, y, z\} \in \mathcal{T}$. The upshot is that no non-trivial $\sigma \in A \rtimes \langle i \rangle$ fixes any $T \in \mathcal{T}$.

By theorem 3, the full automorphism group of this random Cayley graph is isomorphic to $A \rtimes \langle i \rangle$ *whp*. From the preceding discussions, it follows that the random Cayley graph $\Gamma_p(A, S)$, contains a 3-element independent set $\{x, y, z\}$ which is not fixed by any non-trivial automorphism $\sigma \in A \rtimes \langle i \rangle$ *whp*. Color this set with a new color and the rest of the graph using as few colors as possible. This coloring is both proper and distinguishing *whp*. □

5 Random Cayley Graphs on Type II Groups: Proof of Theorem 5

In order to prove Theorem 5, we shall need a lemma that appears in [4]. We state it here, for the sake of completeness.

Lemma 15. *Let C be a proper coloring of the graph G with $\chi(G)$ colors and let C_1 be a color class in C. Let $\mathcal{G}$ be the subgroup of* $\mathrm{Aut}(G)$ *consisting of all automorphisms that fix the color class C_1. For each $A \in \mathcal{G}$, let θ_A denote the total number of distinct orbits induced by the automorphism A in the color class C_1. If for some integer $t \geq 2$,*

$$f(\mathcal{G}) = \sum_{A \in \mathcal{G}} t^{\theta_A - |C_1|} < r$$

where r is the least prime dividing $|\mathcal{G}|$, then $\chi_D(G) \leq \chi(G) + t - 1$. In particular, if $F(C_1) < |C_1| - 2\log_t |\mathcal{G}|$ then this conclusion holds, where $F(C_1)$ is the maximum number of vertices a nontrivial automorphism can fix in C_1.

Before we get to the details of the proof of Theorem 5, we need an additional lemma.

Lemma 16. *Let $A \simeq \mathbb{Z}_2^r \times N$, where N is a non-cyclic group of odd order and let $\Gamma = \Gamma(A, S)$ be a Cayley graph on A. Suppose that* $\mathrm{Aut}(\Gamma) \cong A \rtimes \langle i \rangle$. *If m is the number of elements in A of order at most 2, and $\chi(\Gamma) < \frac{n}{m + 2\log(2n)}$, then $\chi_D(\Gamma) \leq \chi(\Gamma) + 1$.*

Proof. Let us denote $\chi(\Gamma) = \chi$ and let C_1 be a maximum sized color class in a proper coloring of Γ using χ colors, so that $|C_1| \geq n/\chi$.

Observe that a non-trivial automorphism which fixes any vertex of Γ is necessarily of the form (g, i) for some $g \in A$. Moreover, (g, i) fixes a vertex $h \in \Gamma$ if and only if $g = 2h$ in A. Indeed, suppose there exists $0 \neq h_1 \in A$ such that $g = 2h_1$. Then, $0 = 2(h - h_1) = 2h_2$. Therefore $o(h_2) = 2$.

Conversely suppose $o(h_3) = 2$ and write $h_4 = h - h_3$. Then $2h_3 = 0 \implies 2h = 2h_4 = g$. That is $\#\{h \in A : g = 2h\} = \#\{h \in A : 0 = 2h\}$. Thus, any non-trivial automorphism σ fixes at most m vertices in Γ.

Now, following the notation from Lemma 15, we have $\theta_\sigma \leq m + (|C_1| - m)/2$ and hence by the same lemma, we have $f(\mathcal{G}) \leq 2nt^{-\alpha}$ where $\alpha := \frac{n/\chi - m}{2}$. Now observe that

$$t := \lceil (2n)^{\frac{2\chi}{n - m\chi}} \rceil \implies 2n < t^\alpha.$$

Hence there exists a proper $\chi + t - 1$ coloring of Γ that is also distinguishing. In particular, if $\chi < \frac{n}{m + 2\log(2n)}$ we may take $t = 2$, and this proves the lemma. □

Finally we have the corresponding theorem for random Cayley graph $\Gamma_p(A, S)$ for $A \simeq \mathbb{Z}_2^r \times N$ with N being a non-cyclic group of odd order.

Proof of Theorem 5. Let

$$X' := \sum_{\substack{x : 2x = 0 \\ x \neq 0}} \mathbf{1}_{x \in S} \qquad X'' := \sum_{\substack{(x, -x) \\ x \neq -x}} \mathbf{1}_{x, -x \in S}$$

so $|S| = X' + 2X''$. Then X', X'' are binomial random variables with parameters $(m - 1, p)$ and $(\frac{n-m}{2}, p)$ respectively. Then

$$\mathbb{E}(|S|) = (n - 1)p < np.$$

By the concentration of binomial random variables (see theorem 2.1 in [10]) we have

$$\begin{aligned} \mathbb{P}(|S| \geq \mathbb{E}(|S|) + 3t) &\leq \mathbb{P}(X' \geq \mathbb{E}(X') + t) + \mathbb{P}(X'' \geq \mathbb{E}(X'') + t) \\ &\leq \exp\Big(- \frac{t^2}{2((m-1)p + \frac{t}{3})} \Big) + \exp\Big(- \frac{t^2}{2(\frac{n-m}{2}p + \frac{t}{3})} \Big) \end{aligned} \tag{5}$$

Set $t = \frac{2n}{13(m + 2\log 2n)}$. Since $m \ll \frac{n}{\log^2 n}$ it follows that for

$$\frac{25\log^2 n}{n} \leq p < \frac{7}{13(m + 2\log 2n)} < 1 - \frac{25\log^2 n}{n}$$

the right hand side of (5) is at most $e^{-\Omega(\log^2 n)}$, so that *whp* $|S| \leq \frac{13np}{7} < \frac{n}{m + 2\log(2n)}$. Hence by Theorem 3 and lemma 16, and the fact that $\chi(G) \leq \Delta(G) + 1$ for any graph G, it follows that $\chi_D(\Gamma_p) \leq \chi(\Gamma_p) + 1$ *whp*. □

6 Concluding Remarks

1. As emphasized in the introduction, all our results regarding random Cayley graphs hold with probability $1 - n^{-\Omega(\log n)}$. However, if we wish to only prove the same results *asymptotically*

almost surely, (a.a.s) i.e., with probability $1-o(1)$, then improvements on some of the results is not difficult. For instance, Alon proved in [1] that if we pick $k \leq n/2$ subsets uniformly at random and then complete them to inverse-closed sets, then *a.a.s* $\chi(\Gamma(A,S)) \leq O\left(\frac{k}{\log k}\right)$. So for $A \simeq \mathbb{Z}_2^r \times N$ with N a non-cyclic group of odd order with $n^{3/4}\log n \ll m \ll \frac{n}{\log n}$, one can prove by minor modifications, that *a.a.s* $\chi_D(\Gamma_p) \leq \chi(\Gamma_p)+1$ if $\frac{c\log^2 n}{n} \leq p \leq \frac{C\log n}{m+2\log 2n}$ for suitable constants c, C. We skip the details.

2. For non abelian groups A, it is a yet-unsettled conjecture of Babai, Godsil, Imrich, and Lovász (see [3] for details and a proof of the conjecture for nilpotent non-abelian groups), that for any group which is not generalized dihedral, almost surely $\mathrm{Aut}(\Gamma_{1/2}(A,S)) \simeq A$ as $|A| \to \infty$. Thus, for all such graphs it is clear that $\chi_D(G) \leq \chi(G)+1$ since one can pick an arbitrary non-identity element of A, color it using a distinct color, and color the rest of the graph using at most $\chi(G)$ colors. Since A acts regularly, it follows that this coloring is distinguishing as well.

3. Though all the results of this paper establish that $\chi_D(\Gamma) \leq \chi(\Gamma)+1$ holds with high probability, we in fact believe that something stronger is true, at least for random Cayley graphs $\Gamma_{1/2}(A,S)$:

   Conjecture 17. *For a random Cayley graph $\Gamma = \Gamma_{1/2}(A,S)$, we have $\chi_D(\Gamma) = \chi(\Gamma)$ a.a.s.*

   At the moment, we are only able to show the same in certain non-abelian q-groups, for q a large enough prime. Indeed, by some small tweaks to the proof of the main result of [3], one can show that a random Cayley graph $\Gamma = \Gamma_{1/2}(A,S)$ almost surely has full automorphism group isomorphic to A, when A is a nilpotent non-abelian group. Also, one can follow the same line of argument as in [1], to show that $\chi(\Gamma) = \Omega(\frac{n}{\log^2 n})$. Suppose $|A| = q^r$ for a fixed r, and q a sufficiently large prime. If $\phi = \phi_g$ for $g \in A$ is an automorphism that fixes every color class of this coloring, then note that each color class has at least q elements, so that $\chi(\Gamma) \leq q^{r-1}$. But this contradicts the observation that $\chi(\Gamma) = \Omega(\frac{n}{\log^2 n})$ since $q \gg \Omega_r(\log^2 q)$. The same arguments work over a slightly larger range for $p = \Omega(1)$ along the same lines as discussed above, but the more general case remains an open question. It is also conceivable that this conjecture holds over a larger range for p as well.

Acknowledgments

We thank the anonymous referees for their suggestions and comments that have improved the clarity and overall quality of the paper.

References

[1] N. Alon, The chromatic number of random Cayley graphs, *Europ. J. Combin.*, **34** (2013), 1232-1243.

[2] M. O. Albertson and K. L. Collins, Symmetry Breaking in Graphs, *Electron. J. Combin.*, **3** (1996), #R18.

[3] L. Babai and C. Godsil, On the Automorphism Groups of almost all Cayley Graphs, *Europ. J. Combinatorics*, **3** (1982), 9-15.

[4] N. Balachandran and S. Padinhatteeri, $\chi_D(G)$, $|Aut(G)|$, and a variant of the Motion Lemma, *Ars Math. Contemp.*, **12**(1), 2016, 89-109.

[5] Z. Che and K. L. Collins, The Distinguishing Chromatic Number of Kneser Graphs, *Electron. J. Combin.*, **20(1)** (2013), #P23.

[6] K. L. Collins, M. Hovey, A. N. Trenk, Bounds on the Distinguishing Chromatic Number, *Electron. J. Combin.* **16** (2009) #R88.

[7] K. L. Collins and A. N. Trenk, The Distinguishing Chromatic Number, *Electron. J. Combin.*, **13** (2006), #R16.

[8] E. Dobson, P. Spiga and G. Verret, Cayley Graphs on Abelian Groups, *Combinatorica*, **36**(4) (2016), 371-393.

[9] B. Green, On the Chromatic Number of Random Cayley Graphs, `http://arxiv.org/abs/1308.1872`

[10] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, John Wiley & Sons, Inc., New York, 2000.

[11] Á. Seress, The minimal base size of primitive solvable permutation groups, *J. London Math. Soc.* **53**(2) (1996), 243-255.

7 Appendix: Calculations involved in Theorem 4

In order to compute $\Delta := \sum_{D(T)\cap D(U)\neq\emptyset} \mathbb{P}(B_T \wedge B_U)$, we split this sum into three cases, depending on the size of the intersection $D(T) \cap D(U)$. Note that this intersection size is $2, 4$, or 6.

First, fix $T = \{x, y, z\} \in \mathcal{T}$ and suppose $D(T) = D(U)$ for some $U \in \mathcal{T}$. We claim that $U = T$ or $U = -T$. Indeed, write $U = \{u, v, w\} \in \mathcal{T}$ and suppose without loss of generality that $x-y = u-v$; then $v = u-(x-y)$, so it follows (since $U \in \mathcal{T}$) that $U = \{u, u-(x-y), -2u+(x-y)\}$, so that $D(U) = \{\pm(x-y), \pm(3u-(x-y), \pm(3u-2(x-y)\}$. Now by a routine check, it follows that the sets $D(T)$ and $D(U)$ agree if and only if $u = x, -x$ which gives the sets $U = T, -T$ respectively.

In order to count the number of pairs (T, U) with $|D(T) \cap D(U)| = 4$, firstly, set $\mathfrak{T}_1 := \{\pm(x-y), \pm(x+2y)\}$, $\mathfrak{T}_2 := \{\pm(x-y), \pm(2x+y)\}$, and $\mathfrak{T}_3 := \{\pm(x+2y), \pm(2x+y)\}$. Since $(|A|, 3) = 1$, the map $\phi_3(x) = 3x$ is an automorphism of A, so let us denote its inverse by ψ_3. If $D(T) \cap D(U) = \mathfrak{T}_1$, then, noting that the the only admissible values for $u = \psi_3(x-4y), \psi_3(x-2y)$. Similarly, if $D(T) \cap D(U) = \mathfrak{T}_2$, then the only admissible values for u are $\psi_3(2x+y), \psi_3(4x-y)$, and if $D(T) \cap D(U) = \mathfrak{T}_3$, then $u = \psi_3(y-x), \psi_3(4x+5y)$. Table 1 tabulates these more concisely.

$D(U) \cap D(T)$	**U**	**u**	$D(U) \setminus D(T)$
$\{\pm(x-y), \pm(x+2y)\}$	$\{\psi_3(x-4y), \psi_3(-2x-y), \psi_3(x+5y)\}$	$\psi_3(x-4y)$	$\pm 3y$
$\{\pm(x-y), \pm(x+2y)\}$	$\{\psi_3(2x+y), \psi_3(4y-x), \psi_3(-x-5y)\}$	$\psi_3(2x+y)$	$\pm 3y$
$\{\pm(x-y), \pm(2x+y)\}$	$\{\psi_3(4x-y), \psi_3(x+2y), \psi_3(-5x-y)\}$	$\psi_3(4x-y)$	$\pm 3x$
$\{\pm(x-y), \pm(2x+y)\}$	$\{\psi_3(-x-2y), \psi_3(y-4x), \psi_3(5x+y)\}$	$\psi_3(-x-2y)$	$\pm 3x$
$\{\pm(2x+y), \pm(x+2y)\}$	$\{\psi_3(y-x), \psi_3(-4x-5y), \psi_3(5x+4y)\}$	$\psi_3(y-x)$	$\pm(y+2x)$
$\{\pm(2x+y), \pm(x+2y)\}$	$\{\psi_3(4x+5y), \psi_3(x-y), \psi_3(-5x-4y)\}$	$\psi_3(4x+5y)$	$\pm(y+2x)$

Table 1: $|D(T) \cap D(U)| = 4$

Finally, if $|D(T) \cap D(U)| = 2$, then we firstly count the number of $U \in \mathcal{T}$ such that $D(T) \cap D(U) = \{\pm(x-y)\}$. As seen earlier, if $U = \{u, u-(x-y), -2u+(x-y)\}$ then $\pm(x-y) \in D(U)$. However, if u is any of the elements in column 3 of Table 1, then $|D(T) \cap D(U)| = 4$ and if $u \in \{x, -x\}$ then $D(T) = D(U)$. By similarly counting the number of sets U with $D(T) \cap D(U) = \{\pm(y-z)\}$ and $D(T) \cap D(U) = \{\pm(x-z)\}$, it follows that for any $T \in \mathcal{T}$ there are fewer than $3n$ sets U such that $|D(T) \cap D(U)| = 2$, so we have

$$\Delta < 3n|\mathcal{T}|q^5 + 6|\mathcal{T}|q^4 + 2|\mathcal{T}|q^3.$$