COMBINATORIAL THEORY **5 (4)** (2025), #1 combinatorial-theory.org

SUBSETS OF FREE GROUPS WITH DISTINCT DIFFERENCES

Simon R. Blackburn[1], Emma K. A. Smith*[2], and Luke D.J. Stewart*[3]

[1,2,3]*Department of Mathematics, Royal Holloway University of London, Egham, Surrey TW20 0EZ, U.K.*
s.blackburn@rhul.ac.uk , emma.smith.2020@live.rhul.ac.uk , ldjstewart1995@gmail.com

Submitted: Mar 14, 2024; Accepted: Apr 28, 2025; Published: Dec 20, 2025

Abstract. Let F_n be a free group of rank n, with free generating set X. A subset D of F_n is a *Distinct Difference Configuration* if the differences $g^{-1}h$ are distinct, where g and h range over all (ordered) pairs of distinct elements of D. The subset D has diameter at most d if these differences all have word length at most d. When n is fixed and d is large, the paper shows that the largest distinct difference configuration in F_n of diameter at most d has size approximately $(2n-1)^{d/3}$.

Keywords. Difference sets, distinct difference configurations, free groups, combinatorial designs

Mathematics Subject Classifications. 05B10, 20E05

1. Introduction

Let G be a group. A subset D of G is a *Distinct Difference Configuration*, or *DDC*, if the differences $g^{-1}h$ are distinct, where g and h range over all (ordered) pairs of distinct elements of D. For example, when G is the free group F_X on a set X, then $D = X \cup X^{-1}$ is a DDC (because the word $g^{-1}h$ for distinct $g, h \in D$ is always reduced, so g and h can be recovered from the reduced representative of the difference). However, the set $X \cup X^{-1} \cup \{e\}$, where e is the identity element of G, is not a DDC since the difference of x and e and the difference of e and x^{-1} are equal for any element $x \in X$. As another example of a DDC, in a finite group: the subset $\{1, 2, 4\}$ is a DDC in the additive group of integers modulo 7.

Subsets of abelian groups with distinct differences have been studied for many decades. For example, in 1938 Singer [Sin38] showed that if q is a prime power, then there exists a *perfect difference set of order* $q+1$ (a set of $q+1$ integers whose q^2+q differences are distinct modulo q^2+q+1); see [She06], where the term *modular Golomb ruler* is used. Sidon sets, namely sets of positive integers whose pairwise sums are distinct, have been studied since

---

*Research supported by UKRI and EPSRC as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (Grant Ref. EP/SO21817/1).

the 1930s [Sid32], originally motivated by a problem in Fourier series. In abelian groups, Sidon sets and distinct difference configurations are equivalent notions [O'B04]. The combined results of Erdős and Turán [ET41] and of Singer [Sin38] demonstrate that the maximum number of elements in a Sidon set contained in the interval $[1, x]$ is at least $(1-\epsilon)\sqrt{x}$ (for all ϵ and large enough x) and is at most $\sqrt{x}+O(x^{1/4})$. This result was pointed out by both Chowla [Cho44] and Erdős [Erd44] independently [O'B04].

Difference sets, namely subsets D of a group G such that every non-identity element of G occurs an equal number of times as the difference of elements of D, have been intensively studied in both abelian and non-abelian cases [DJ06]. Many other variants have been studied (motivated by design theory or other applications), for example Costas arrays [WCS23], Golomb rulers [Dra09], difference families [RJRA06] and difference matrices [Col06].

The results of Erdős–Turán and Singer can be thought of as providing bounds on the cardinality of a distinct difference configuration $D \subseteq \mathbb{Z}$ of bounded diameter (so the distance $|h-g|$ between any two elements $g, h \in D$ is small). The natural analogue of diameter for general groups can be defined in terms of a Cayley graph of the group as follows. Let G be a group and let X be a generating set for G. The Cayley graph of G with respect to X is the (regular) graph whose nodes are labelled by elements of G, with an edge from g to gx for all $x \in X \cup X^{-1}$. The *distance* $\operatorname{dist}(g, h)$ between g and h is defined as the length of a shortest path between the nodes labelled g and h. Alternatively, the distance between g and h could be defined to be the smallest non-negative integer ℓ such that $h = gy_1y_2\cdots y_\ell$, where $y_1, y_2, \ldots, y_\ell \in X \cup X^{-1}$. Note that the distance function satisfies the triangle inequality and that $\operatorname{dist}(g, h) = \operatorname{dist}(e, g^{-1}h)$. For a subset $D \subseteq G$, the *diameter* of D is the minimum integer d such that $\operatorname{dist}(g, h) \leqslant d$ for all $g, h \in D$ (if this integer exists).

For a group G with a finite generating set X of cardinality n, it is natural to ask what is the maximum cardinality m of a DDC with diameter d. The work of Erdős–Turán and Singer implies that $m = \Theta(\sqrt{d})$ when $G = \mathbb{Z}$ and $X = \{1\}$. (Recall that if α and β are positive real functions of a positive integer d, we write $\alpha = \Theta(\beta)$ to mean that there exist positive constants c_1 and c_2, independent of d, such that $c_1\beta \leqslant \alpha \leqslant c_2\beta$ whenever d is sufficiently large.) Blackburn et al. [BEMP10, Theorem 9, Corollary 27] show that when $G = \mathbb{Z}^2$ and $X = \{(1,0),(0,1)\}$ then $m = \Theta(d)$. Stewart [Ste23, Chapter 8] shows that when $G = \mathbb{Z}^n$ and X is the standard generating set of size n then $m = \Theta(d^{n/2})$. To understand these results, we note that a DDC of diameter d and cardinality m gives rise to $m(m-1)$ distinct differences, all lying at distance at most d from the identity e. Thus, $m(m-1) \leqslant |B_d(e)|$, where $B_d(e)$ is the *ball of radius* d *about* e (namely the set of all elements of G at distance at most d from e). Since $|B_d(e)| = \Theta(d^n)$ when $G = \mathbb{Z}^n$, these results say that $m = \Theta(\sqrt{|B_d(e)|})$ in the free abelian group of rank 1, 2 and n respectively. This can be interpreted as saying that the bound $m(m-1) \leqslant |B_d(e)|$ is an important restriction on the size of a DDC of diameter d in these groups.

In this paper, we aim to investigate distinct difference configurations of fixed diameter when the group G is a free (non-abelian) group of finite rank. A free group of rank n is a group generated by a set X with cardinality n and is denoted either F_X or F_n depending on the context. Every group element is a reduced word in these generators and their inverses ($X \cup X^{-1}$), with no defining relations other than those required by group axioms. (A word is reduced if xx^{-1} and $x^{-1}x$ do not occur as consecutive subwords, for any $x \in X$.) The Cayley graph of a free group rank n forms a regular infinite tree of degree $2n$.

The motivation for considering the free group in this paper is four-fold: First, solving the problem for a free group of rank n has implications for all n-generator groups (see the discussion in Section 4). Second, the free group is a natural group to consider when moving to the non-abelian case (in analogy to the free abelian cases considered previously). Third, we believe the results are surprising. Our final motivation comes from an application to key distribution in wireless sensor networks similar to the scheme introduced in [BEMP08], which considered sensors that are physically arranged in a grid. In the grid-based application, the relevant word metric in the group is a good approximation for the Euclidean distance between the sensors; the distinct difference condition is required so that a pair of communicating sensors share exactly one key. We can envisage applications where the grid is replaced by a regular tree which represents wired communication rather than a wireless environment.

This paper proves the following theorem.

Theorem 1.1. *Let F_X be a free group, freely generated by a set X of cardinality n, where $n \geqslant 2$. Let $m(n, d)$ be the maximum cardinality of a DDC of diameter at most d in F_X. As $d \to \infty$ with n fixed, then*

$$m(n, d) = (2n - 1)^{d/3+O(\log d)}$$

(*where the implicit constants might depend on n*).

In fact, we will show an upper bound of the form $m(n, d) \leqslant (2n - 1)^{d/3+O(1)}$. We comment that our lower bound is probabilistic.

Roughly speaking the theorem says that, in the free group, $m(n, d) \approx (2n - 1)^{d/3}$ when n is fixed. This result is rather surprising: the ball $B_d(e)$ of radius d about the identity in the free group has cardinality

$$1 + \sum_{i=1}^{d} 2n(2n - 1)^{i-1} = \Theta((2n - 1)^d)$$

and so, extrapolating from the results on the free abelian case above, you might guess that the right answer should be $m(n, d) \approx \sqrt{|B_d(e)|} \approx (2n-1)^{d/2}$. (You could prove an upper bound of this form by using the inequality $m(m-1) \leqslant |B_d(e)|$.) Theorem 1.1 shows that in fact the correct order of magnitude of $m(n, d)$ is much smaller than this, so there are more restrictive bounds on the cardinality of a DDC of diameter d in the free group than the bound $m(m - 1) \leqslant |B_d(e)|$.

How big is a subset of diameter d in the free group, irrespective of it having distinct differences? For any element g in a group G, it is easy to see that the ball $B_r(g)$ of radius r and centre g in G is a subset of G of diameter at most $2r$. When G is the free group F_X with free generating set X and when d is even, every subset D of F_X of diameter d is contained in a ball of radius $d/2$. To see this, choose a pair of elements of D at distance d and let g be the element of F_X that is equidistant between them. Since D has diameter d, and F_X is a tree, every element of D lies at distance at most $d/2$ from g. Hence D is contained in $B_{d/2}(g)$. So a subset of F_X of diameter d has cardinality at most

$$|B_{d/2}(g)| = 1 + \sum_{i=1}^{d/2} 2n(2n - 1)^{i-1} = \Theta((2n - 1)^{d/2})$$

when d is even; this bound is tight since $B_{d/2}(g)$ has diameter d. When d is odd, we may similarly argue that a subset of F_X of diameter d has cardinality at most $|B_{(d+1)/2}(g)| = \Theta((2n-1)^{d/2})$. (This bound is no longer tight, as $B_{(d+1)/2}(g)$ does not have diameter d. A tight bound is not hard to prove; the analogue of the ball of radius $d/2$ in this situation is the union of two balls of radius $\lfloor d/2 \rfloor$ whose centres are at distance 1.) We conclude that the largest subsets of diameter d in F_X are of size approximately $(2n-1)^{d/2}$, which (by Theorem 1.1) is much larger than the size $m(n,d)$ of a DDC of diameter d of maximal cardinality.

We have now seen two elementary arguments showing that $m(n,d)$ grows no faster than $(2n-1)^{d/2}$ (approximately), namely using the bound $m(m-1) \leqslant |B_d(e)|$ or using the above bound on the cardinality of diameter d subsets. Now we turn our attention to lower bounds. The following explicit construction of a DDC leads to a lower bound on $m(n,d)$ (weaker than the bound implied by Theorem 1.1).

Construction 1.2. *Let d be divisible by 4 and let R be the set of reduced words of length $d/4$. For a reduced word w, let $\operatorname{rev}(w)$ be the reverse of w (so $\operatorname{rev}(w)$ is a reduced word, with symbols listed in the opposite order to w). For any $w \in R$, the concatenation $w \operatorname{rev}(w)$ is a reduced word of length $d/2$. Define $D = \{w \operatorname{rev}(w) : w \in R\}$.*

The set D in Construction 1.2 is contained within $B_{d/2}(e)$, where e is the identity element, and so D has diameter at most d. Furthermore, the following argument shows that all differences in D are distinct. Suppose that $y, y' \in D$ with $y \neq y'$. Then $y = w \operatorname{rev}(w)$ and $y' = w' \operatorname{rev}(w')$ for distinct $w, w' \in R$. The difference $(y')^{-1}y$ is of the form $\operatorname{rev}(w')^{-1}(w')^{-1}w \operatorname{rev}(w)$. Since w, w' are distinct and reduced, the expression $(w')^{-1}w$ does not reduce to the identity, and so the reduced form of $(y')^{-1}y$ begins with $d/4$ symbols representing $\operatorname{rev}(w')^{-1}$ and ends with $d/4$ symbols representing $\operatorname{rev}(w)$. So $\operatorname{rev}(w)$ and $\operatorname{rev}(w')$, and hence y and y', are determined by the reduced form of $(y')^{-1}y$. Thus the differences are all distinct, and D is a DDC. Since $|D| = |R| = 2n(2n-1)^{d/4-1}$, we have constructed a DDC of diameter d and cardinality approximately equal to the cardinality of the ball $B_d(e)$ raised to the power $1/4$.

A second lower bound can be found by considering the work of Babai and Sós who show in [BS85] that any subset W of a group contains a subset $V \subseteq W$ with cardinality $|V| = (c + o(1))|W|^{1/3}$ (where $c \approx 0.47$) such that $x^{-1}y \neq z^{-1}w$ for any $x, y, z, w \in V$ of which at least three are different. If we let $W = |B_{\lfloor d/2 \rfloor}(e)|$ and apply this result along with our Lemma 3.1, then we see that there exists a set with cardinality $(c + o(1))(2n-1)^{d/6}$ which has distinct differences and diameter at most d. Therefore we get a lower bound on $m(n,d)$ which is weaker than both Construction 1.2 and Theorem 1.1.

The remainder of the paper is structured as follows. In Section 2 we prove the upper bound of Theorem 1.1. In Section 3 we provide a probabilistic argument to establish the lower bound in Theorem 1.1 (finishing the proof of the theorem). Finally, in Section 4 we provide some commentary, and list some open problems.

2. An upper bound

In this section we provide an upper bound on the maximum cardinality $m(n,d)$ of a DDC with diameter d contained in the free group of rank n. This gives the upper bound in Theorem 1.1.

We require the following definitions. Let F_X be a free group, finitely generated by a set X of cardinality n. Let D be a DDC in F_X with diameter d. Recall that for even d, the set D is contained in a ball of radius $d/2$ with centre an element $g \in F_X$, denoted $B_{d/2}(g)$. Indeed, we may assume (for even d) that $D \subseteq B_{d/2}(e)$ because we may replace D by $g^{-1}D$ without altering the distinct difference property or diameter. Similarly, for odd d, we may assume that $D \subseteq B_{(d+1)/2}(e)$.

Define the *sphere of radius r about e*, denoted $S_r(e)$, by $S_r(e) = B_r(e) \setminus B_{r-1}(e)$. Equivalently, $S_r(e)$ denotes all elements at distance exactly r from e, the 'outer' elements of the ball. For every $x \in B_r(e)$, define $D_x = \{x' \colon xx' \in D, xx' \text{ is reduced}\}$. So D_x consists of the strings following x in the reduced words representing elements of D.

Lemma 2.1. *Let $D \subseteq S_r(e)$ where r is a positive integer. If D is a DDC, then*

$$|D_x \cap D_y| \leqslant 1 \textit{ for all distinct } x, y \in B_{r-1}(e).$$

Proof. Assume that for some $x, y \in B_{r-1}(e)$, where $x \neq y$, we have $|D_x \cap D_y| \geqslant 2$. Then there must exist $z, w \in D_x$ and $z, w \in D_y$, where $z \neq w$. Therefore, there must be elements $a = xz, b = xw, u = yz, v = yw$ that are reduced, distinct elements of D. Then, $a^{-1}b = z^{-1}x^{-1}xw = z^{-1}y^{-1}yw = u^{-1}v$, and so D does not have pairwise distinct differences. Therefore, if D is a DDC, then $|D_x \cap D_y| \leqslant 1$ for all $x, y \in B_{r-1}(g)$ where $x \neq y$. ☐

Lemma 2.1 provides a necessary condition for a set D contained in a sphere to be a DDC. This condition is in fact both necessary and sufficient: see [Ste23, Theorem 6.0.5]. We now prove the main theorem of this section.

Theorem 2.2. *Let F_X be a free group, freely generated by a set X of cardinality n, where $n \geqslant 2$. Let $m(n, d)$ be the maximum cardinality of a DDC of diameter d in F_X. As $d \to \infty$ with n fixed, there exists a positive constant c (independent of d, but depending on n) such that*

$$m(n, d) \leqslant c(2n-1)^{d/3}$$

for all sufficiently large d.

In fact, we show that

$$|D| \leqslant \frac{2n(4n^2-3n+1)}{(2n-1)^{2/3}((2n-1)^{2/3}-1)} \cdot (2n-1)^{d/3}.$$

Proof. Let $D \subseteq F_X$ be a DDC of diameter d. Without loss of generality, replacing D by $g^{-1}D$ if necessary for some $g \in F_X$, we may assume that $D \subseteq B_{\lceil d/2 \rceil}(e)$. Let j be a non-negative integer and let $D^{(j)}$ denote the set $D \cap S_j(e)$. Then $D = \bigcup_{j=0}^{\lceil d/2 \rceil} D^{(j)}$. Note that $|D^{(0)}| \leqslant 1$, and therefore

$$|D| \leqslant 1 + \sum_{j=1}^{\lceil d/2 \rceil} |D^{(j)}|. \tag{2.1}$$

We now prove an upper bound on the cardinality of the sets $D^{(j)}$. If k_j is a non-negative integer strictly less than j, then it is not difficult to see that $D^{(j)} = \bigcup_{x \in S_{k_j}(e)} x \cdot {D^{(j)}}_x$, where ${D^{(j)}}_x = \{x' \colon xx' \in D^{(j)}, xx' \text{ is reduced}\}$, as in Lemma 2.1. We choose k_j to be $\lfloor j/3 \rfloor$. The sets $x \cdot {D^{(j)}}_x$ are distinct for each $x \in S_{\lfloor j/3 \rfloor}(e)$, so we have

$$|D^{(j)}| = \sum_{x \in S_{\lfloor j/3 \rfloor}(e)} |{D^{(j)}}_x|. \tag{2.2}$$

By the inclusion-exclusion principle, we have

$$\left| \bigcup_{x \in S_{\lfloor j/3 \rfloor}(e)} {D^{(j)}}_x \right| \geqslant \sum_{x \in S_{\lfloor j/3 \rfloor}(e)} |{D^{(j)}}_x| - \sum_{\substack{x,y \in S_{\lfloor j/3 \rfloor}(e),\\ x \neq y}} \left|{D^{(j)}}_x \cap {D^{(j)}}_y\right|. \tag{2.3}$$

Combining inequality (2.1), equation (2.2) and inequality (2.3), we have

$$|D| \leqslant 1 + \sum_{j=1}^{\lceil d/2 \rceil} \left(\left| \bigcup_{x \in S_{\lfloor j/3 \rfloor}(e)} {D^{(j)}}_x \right| + \sum_{\substack{x,y \in S_{\lfloor j/3 \rfloor}(e),\\ x \neq y}} \left|{D^{(j)}}_x \cap {D^{(j)}}_y\right| \right). \tag{2.4}$$

For all $x \in S_{\lfloor j/3 \rfloor}(e)$, every element in ${D^{(j)}}_x$ has length $j - \lfloor j/3 \rfloor$. Therefore,

$$\bigcup_{x \in S_{\lfloor j/3 \rfloor}(e)} {D^{(j)}}_x \subseteq S_{j - \lfloor j/3 \rfloor}(e).$$

As $j - \lfloor j/3 \rfloor \leqslant 2j/3 + 1$, we have

$$\left| \bigcup_{x \in S_{\lfloor j/3 \rfloor}(e)} {D^{(j)}}_x \right| \leqslant 2n(2n-1)^{2j/3}.$$

Each set $D^{(j)}$ is a DDC where every element has equal length j. Lemma 2.1 tells us that for every j, we have $|{D^{(j)}}_x \cap {D^{(j)}}_y| \leqslant 1$ for all distinct $x, y \in S_{\lfloor j/3 \rfloor}(e)$. Using the fact that

$$\binom{|S_{\lfloor j/3 \rfloor}(e)|}{2} < \tfrac{1}{2} \left(2n(2n-1)^{\lfloor j/3 \rfloor - 1} \right)^2,$$

and $2\lfloor j/3 \rfloor \leqslant 2j/3$, inequality (2.4) now becomes

$$|D| \leqslant 1 + \sum_{j=1}^{\lceil d/2 \rceil} \left(2n(2n-1)^{2j/3} + 2n^2(2n-1)^{2j/3-2} \right). \tag{2.5}$$

We can rearrange inequality (2.5) to get

$$|D| \leqslant 1 + \frac{2n(4n^2 - 3n + 1)}{(2n-1)^2} \sum_{j=1}^{\lceil d/2 \rceil} (2n-1)^{2j/3}. \tag{2.6}$$

The summation in (2.6) forms a geometric sequence, and as $\lceil d/2 \rceil \leqslant d/2+1$ we find

$$|D| \leqslant 1 + \frac{2n(4n^2-3n+1)}{(2n-1)^2} \cdot \frac{(2n-1)^{2/3}}{(2n-1)^{2/3}-1} \cdot ((2n-1)^{(2/3)(d/2+1)}-1). \tag{2.7}$$

We rewrite inequality (2.7) to see

$$|D| \leqslant 1 - \frac{2n(4n^2-3n+1)}{(2n-1)^{4/3}((2n-1)^{2/3}-1)} + \frac{2n(4n^2-3n+1)}{(2n-1)^{2/3}((2n-1)^{2/3}-1)} \cdot (2n-1)^{d/3}.$$

Since

$$\frac{2n(4n^2-3n+1)}{(2n-1)^{4/3}((2n-1)^{2/3}-1)} \geqslant 1,$$

we get the desired bound of

$$|D| \leqslant \frac{2n(4n^2-3n+1)}{(2n-1)^{2/3}((2n-1)^{2/3}-1)} \cdot (2n-1)^{d/3}. \qquad \square$$

Theorem 2.2 proves the upper bound in Theorem 1.1.

3. A lower bound

In this section we prove a probabilistic result which forms the lower bound on $m(n,d)$, the maximum cardinality of a DDC of diameter d in the free group of rank n.

Let F_X be a free group, freely generated by a set X of cardinality n, where $n \geqslant 2$. The sphere $S_r(e)$ of radius r centred at the identity e is a subset of F_X with diameter $2r$. We show the existence of a large DDC in this sphere. Firstly, we prove that any three-element subset of the free group whose elements have equal length must have pairwise distinct differences.

Lemma 3.1. *Let F_X be a free group, freely generated by a set X of cardinality n, where $n \geqslant 2$. Let r be a positive integer. If D is a subset of $S_r(e)$ with cardinality 3 then D is a DDC.*

Proof. Write $D = \{a,b,c\}$ where $a,b,c \in S_r(e)$ are distinct elements of F_X of length r. Assume, for a contradiction, that D is not a DDC. Then two differences in D agree. If these differences involve just two elements, a and b say, then we must have $a^{-1}b = b^{-1}a$. But this implies that $(ab^{-1})^2 = e$. Since F_X has no elements of order 2, we see that $ab^{-1} = e$ and so $a = b$. This contradicts the fact that a and b are distinct. So all three elements must be involved in our two agreeing differences in D. Up to relabelling, either $a^{-1}b = a^{-1}c$, or $a^{-1}b = c^{-1}a$. If $a^{-1}b = a^{-1}c$, then by left-multiplying by a we see $b = c$ which is again a contradiction. So we may assume that $a^{-1}b = c^{-1}a$ and a,b,c are distinct.

If $a^{-1}b = c^{-1}a$, then the reduced words $a^{-1}b$ and $c^{-1}a$ must have the same length. If there is no reduction, then by comparing letters we see $a = c$ which is a contradiction. So there must exist a positive integer $k \leqslant r$ such that the reduced words $a^{-1}b$ and $c^{-1}a$ both have length $2r-2k$. Write a_i, b_i and c_i for the ith letter in the words a, b and c respectively. Then, we have $a_1 \cdots a_k = b_1 \cdots b_k$. By comparing letters on the right hand side of the reduced words corresponding to $a^{-1}b$ and $c^{-1}a$, we also get $b_{k+1} \cdots b_r = a_{k+1} \cdots a_r$. But then $a = b$ which is a contradiction. $\square$

Lemma 3.1 tells us that when considering subsets of the free group where all elements have the same length, if the subset is not a distinct difference configuration then the repeated difference must arise from the pairwise differences of four distinct elements. We now prove the lower bound.

Theorem 3.2. *Let F_X be a free group, freely generated by a set X of cardinality n, where $n \geqslant 2$. Let $m(n,d)$ be the maximum cardinality of a DDC of diameter at most d in F_X. As $d \to \infty$ with n fixed,*

$$m(n,d) \geqslant (2n-1)^{d/3+O(\log(d))}.$$

Proof. We will show that when d is even, we have

$$m(n,d) \geqslant 2n(2n-1)^{d/3-(4/3)\log_{2n-1}(d/3)-5}. \tag{3.1}$$

The left hand side of inequality (3.1) implies a lower bound of the form $(2n-1)^{d/3+O(\log(d))}$. Therefore once we have established inequality (3.1) for d even, the theorem is proved for when d is even. If d is odd, then $m(n,d) \geqslant m(n,d-1)$ where $d-1$ is even. Hence (3.1) shows the theorem also holds when d is odd. It therefore suffices to prove inequality (3.1) where we may assume that d is even.

Let γ be a rational number so that $\frac{d}{3}-\gamma$ is a positive integer. We will choose the specific value of γ later (which will be logarithmic in d). We construct a randomised set as follows.

Let $V = S_{d/3-\gamma}(e)$, and let $W = S_{d/6+\gamma}(e)$. For all $v \in V$, choose $w_v \in W$, uniformly and independently at random so that vw_v is reduced. Note that there are $2n(2n-1)^{d/6+\gamma}$ options for each w_v. Let $D = \{vw_v \mid v \in V\}$ be the resulting random subset of words in F_X.

Note that $|D| = |V| = 2n(2n-1)^{d/3-\gamma-1}$, because $vw_v \neq v'w_{v'}$ when $v \neq v'$. Also, $D \subseteq S_{d/2}(e)$ because vw_v is always reduced. The diameter of D is therefore less than or equal to d.

If D is a set constructed as previously described, we wish to know how many duplicated differences we would expect. All elements in D have equal length $\frac{d}{2}$ and so Lemma 3.1 tells us that if there is a repeated difference, then there must be four distinct elements u, v, x, y in V such that $(uw_u)^{-1}(vw_v) = (xw_x)^{-1}(yw_y)$.

Let $A_{u,v,x,y}$ be the event that $(uw_u)^{-1}(vw_v) = (xw_x)^{-1}(yw_y)$, and let $I_{u,v,x,y}$ be the indicator random variable for event $A_{u,v,x,y}$. Let $\mathbb{P}_{u,v,x,y}$ be the probability that $I_{u,v,x,y} = 1$.

Define $\eta(D) = \sum_{(u,v,x,y)} \mathbb{P}_{u,v,x,y}(D)$, where the sum is over ordered quadruples (u,v,x,y) of distinct elements of V. By linearity of expectation, $\eta(D)$ is the expected number of bad events that occur. We aim to show that

$$\eta(D) \leqslant (d/3-1)2n(2n-1)^{d/3-4\gamma-1}. \tag{3.2}$$

This suffices to prove the theorem, by the following argument. There exists an outcome $D^* \subseteq S_{d/2}(e)$ where the number of repeated differences is at most $\eta(D)$. By removing at most $\eta(D)$ elements from D^* (one element in each bad event), we produce a subset D' which is a DDC of diameter at most d, and has cardinality at least $|D^*| - \eta(D)$. Hence $m(n,d) \geqslant |D^*| - \eta(D)$. The inequality (3.2) therefore implies

$$m(n,d) \geqslant 2n(2n-1)^{d/3-\gamma-1} - (d/3-1)2n(2n-1)^{d/3-4\gamma-1}.$$

Now we choose our rational number γ to be such that $\frac{d}{3} - \gamma$ is a positive integer and

$$\frac{1}{3}\log_{2n-1}(d/3) \leqslant \gamma \leqslant \frac{1}{3}\log_{2n-1}(d/3) + 1.$$

Using the lower bound on γ, we have $d/3 \leqslant (2n-1)^{3\gamma}$ and therefore

$$m(n,d) \geqslant 2n(2n-1)^{d/3-4\gamma-1}.$$

Then using the upper bound on γ we see that

$$m(n,d) \geqslant 2n(2n-1)^{d/3-(4/3)\log_{2n-1}(d/3)-5},$$

proving inequality (3.1). So the theorem follows, once we have established (3.2). We now show that this inequality holds.

Assume that for some distinct $u, v, x, y \in V$, we have

$$(uw_u)^{-1}(vw_v) = (xw_x)^{-1}(yw_y).$$

As u, v, x, y are distinct, there must be some cancellation, which must be of equal length on both sides. Therefore for some (strictly) positive integer k, we have

$$|(uw_u)^{-1}(vw_v)| = |(xw_x)^{-1}(yw_y)| = d - 2k.$$

As $u \neq v$ and $x \neq y$, we have $k < d/3 - \gamma$. In other words, for some $0 < k < d/3 - \gamma$ the following conditions hold:

$$u_1 \dots u_k = v_1 \dots v_k, \tag{3.3}$$
$$x_1 \dots x_k = y_1 \dots y_k, \tag{3.4}$$
$$u_{k+1} \dots u_{d/3-\gamma} = x_{k+1} \dots x_{d/3-\gamma}, \tag{3.5}$$
$$v_{k+1} \dots v_{d/3-\gamma} = y_{k+1} \dots y_{d/3-\gamma}, \tag{3.6}$$
$$u_{k+1} \neq v_{k+1}, \tag{3.7}$$
$$x_{k+1} \neq y_{k+1}. \tag{3.8}$$

Note that, for a given choice of u, v, x and y, conditions (3.3) to (3.8) are satisfied for at most one value of k. If u, v, x and y are such that these conditions are never satisfied, whatever the value of k, then $\mathbb{P}_{u,v,x,y}(D) = 0$. Otherwise, $\mathbb{P}_{u,v,x,y}(D)$ is equal to the probability that $w_u = w_x$ and $w_v = w_y$ and so $\mathbb{P}_{u,v,x,y}(D) \leqslant (2n-1)^{-2(d/6+\gamma)}$. Hence

$$\eta(D) \leqslant \sum_{k=1}^{d/3-\gamma} \sum_{u,v,x,y} (2n-1)^{-2(d/6+\gamma)}, \tag{3.9}$$

where the inner sum runs over all distinct $u, v, x, y \in V$ that satisfy conditions (3.3) to (3.8). There are at most $d/3 - 1$ choices for the value of k in (3.9). Fix a value of k. There are $2n(2n-1)^{d/3-\gamma-1}$ choices for u, and then $(2n-1)^{d/3-\gamma}$ choices for y (as $y_{k+1} \neq u_{k+1}$

by (3.5) and (3.8)). The choices of u and y, the value of k, and the conditions (3.3) to (3.6) determine v and x. So there are at most $2n(2n-1)^{2d/3-2\gamma-1}$ terms in the inner sum of (3.9). Hence (3.9) implies

$$\eta(D) \leqslant (d/3-1)2n(2n-1)^{2d/3-2\gamma-1}(2n-1)^{-2(d/6+\gamma)},$$

which proves the inequality (3.2) as required. □

Theorem 3.2 proves the lower bound of Theorem 1.1. Combined with Theorem 2.2, which forms the upper bound, this completes the proof of Theorem 1.1.

4. Discussion

1. It would be interesting to tighten our bounds on $m(n,d)$, the largest DDC in F_n of diameter at most d, and to remove the probabilistic nature of our lower bound:

   Open Problem 4.1. Is there a good explicit construction for a large DDC of diameter d in F_n?

   Open Problem 4.2. As $d \to \infty$ with n fixed, is it the case that $m(n,d) = (2n-1)^{d/3+O(1)}$?

2. The problem of determining $m(n,d)$ when d is fixed is also interesting. Stewart [Ste23] shows that $m(n,2) = 2n$, that $m(n,3) = 2n+1$, and $m(n,4) = 2\sqrt{2}n^{3/2} + o(n^{1.3})$. (The exponent of the error term comes from known results on the gaps between primes.)

3. Our upper bound on $m(n,d)$ has implications for all finitely generated groups. Indeed, we have the following theorem:

   Theorem 4.3 (Stewart [Ste23])**.** *Let G be a finitely generated group with finite generating set $\{g_1, g_2, \ldots, g_n\}$ of cardinality n. Let D be a DDC in G of diameter at most d. Then $|D| \leqslant m(n,2d)$, where $m(n,2d)$ is the maximum size of a DDC of diameter at most $2d$ in the free group F_n of rank n.*

   Proof. Let $\{x_1, x_2, \ldots, x_n\}$ be a free generating set for F_n. Let $\phi : F_n \to G$ be the (unique) homomorphism such that $\phi(x_i) = g_i$ for $i \in \{1,2,\ldots,n\}$. For a DDC $D = \{h_1, h_2, \ldots, h_m\}$ in G of cardinality m and of diameter at most d, define a DDC $\hat{D} = \{\hat{h}_1, \hat{h}_2, \ldots, \hat{h}_m\} \subseteq F_n$ as follows. Set $\hat{h}_1 \in F_n$ to be any element such that $\phi(\hat{h}_1) = h_1$. For $i > 1$, define $\hat{h}_i \in F_n$ to be any element such that $\phi(\hat{h}_i) = h_i$ and such that $\mathrm{dist}(\hat{h}_1, \hat{h}_i) \leqslant d$. We see that $\hat{D}$ is a DDC in F_n of cardinality $|D|$ and diameter at most $2d$. Hence $|D| \leqslant m(n,2d)$ and the theorem follows. □

   Open Problem 4.4. Let G be a finitely generated group with a finite generating set of cardinality n. Let D be a DDC in G of diameter at most d. Is it the case that $|D| \leqslant m(n,d)$?

We note that this problem cannot be solved by naively pulling a DDC in G back into the free group: in the notation of the theorem above, there are examples of subsets $D \subseteq G$ of diameter d such that any preimage $\hat{D} \subseteq F_n$ with $\phi(\hat{D}) = D$ always has diameter greater than d.

4. Let G be a group generated by a finite set X. We have defined the difference between two elements g and h in a group G as $g^{-1}h$. We could define this as the *right difference* between g and h, and define the equally natural *left difference* between g and h as gh^{-1}. So a *left distinct difference configuration* is a subset D whose left differences are distinct. This alternative definition of a distinct difference configuration is commonly used in the literature. We define the *left distance* between g and h as the length of the shortest expression of gh^{-1} as a product of elements in $X \cup X^{-1}$, and the *left diameter* of D as the largest left distance between a pair of elements in D. Note that whilst a right distinct difference configuration of right diameter d is always a left distinct difference configuration, it might not have left diameter d. (For example, the subset $D = \{x_1x_2, x_1x_3\} \subset F_3$ has right diameter 2 but left diameter 4.) However, it is not hard to prove that D is a (right) distinct difference configuration of diameter d if and only if $D^{-1} := \{g^{-1} : g \in D\}$ is a left distinct difference configuration of left diameter d. Therefore, our results hold for both the left and right variations of the definitions.

Acknowledgements

We would like to thank the referees for their useful suggestions.

References

[BEMP08] Simon Blackburn, Tuvi Etzion, Keith Martin, and Maura Paterson. Efficient key predistribution for grid-based wireless sensor networks. In *Information Theoretic Security. Lecture Notes in Computer Science 5155*, pages 54–69. Springer Berlin Heidelberg, 08 2008. `doi:10.1007/978-3-540-85093-9_6`.

[BEMP10] Simon R. Blackburn, Tuvi Etzion, Keith M. Martin, and Maura B. Paterson. Two-dimensional patterns with distinct differences—constructions, bounds, and maximal anticodes. *IEEE Trans. Inform. Theory*, 56(3):1216–1229, 2010. `doi:10.1109/TIT.2009.2039046`.

[BS85] László Babai and Vera T. Sós. Sidon sets in groups and induced subgraphs of Cayley graphs. *European J. Combin.*, 6(2):101–114, 1985. `doi:10.1016/S0195-6698(85)80001-9`.

[Cho44] S. Chowla. Solution of a problem of Erdős and Turán in additive-number theory. *Proc. Nat. Acad. Sci. India Sect. A*, 14:1–2, 1944.

[Col06] Charles J. Colbourn. Difference matrices. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs, 2nd edition*, pages 411–419. CRC Press, Boca Raton, 2006. `doi:10.1201/9781420010541`.

[DJ06] Ken W. Smith Dieter Jungnickel, Alexander Pott. Difference sets. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs, 2nd edition*, pages 419–435. CRC Press, Boca Raton, 2006. `doi:10.1201/9781420010541`.

[Dra09] Konstantinos Drakakis. A review of the available construction methods for Golomb rulers. *Adv. Math. Commun.*, 3(3):235–250, 2009. `doi:10.3934/amc.2009.3.235`.

[Erd44] P. Erdős. On a problem of Sidon in additive number theory and on some related problems. Addendum. *J. London Math. Soc.*, 19:208, 1944. `doi:10.1112/jlms/19.76\_Part\_4.208`.

[ET41] P. Erdős and P. Turán. On a problem of Sidon in additive number theory, and on some related problems. *J. London Math. Soc.*, s1-16(4):212–215, 1941. `doi:10.1112/jlms/s1-16.4.212`.

[O'B04] Kevin O'Bryant. A complete annotated bibliography of work related to Sidon sequences. *Electron. J. Combin.*, DS11:39, 2004. `doi:10.37236/32`.

[RJRA06] Marco Buratti R. Julian R. Abel. Difference families. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs, 2nd edition*, pages 392–410. CRC Press, Boca Raton, 2006. `doi:10.1201/9781420010541`.

[She06] James B. Shearer. Difference triangle sets. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs, 2nd edition*, pages 436–440. CRC Press, Boca Raton, 2006. `doi:10.1201/9781420010541`.

[Sid32] S. Sidon. Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen. *Math. Ann.*, 106(1):536–539, 1932. `doi:10.1007/BF01455900`.

[Sin38] James Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938. `doi:10.2307/1990067`.

[Ste23] Luke Stewart. *Distinct Difference Configurations in Groups*. PhD thesis, Royal Holloway, University of London, 2023.

[WCS23] Lutz Warnke, Bill Correll, Jr., and Christopher N. Swanson. The density of Costas arrays decays exponentially. *IEEE Trans. Inform. Theory*, 69(1):575–581, 2023. `doi:10.1109/tit.2022.3202507`.