

Journal of Integer Sequences, Vol. 20 (2017), Article 17.8.1

Bases in Dihedral and Boolean Groups

Volodymyr Gavrylkiv Vasyl Stefanyk Precarpathian National University Department of Algebra and Geometry Shevchenko str., 57 Ivano-Frankivsk Ukraine vgavrylkiv@gmail.com

Abstract

A subset B of a group G is called a *basis* of G if $G = B^2$. The smallest cardinality of a basis of G is called the *basis size* of G. We prove upper bounds for basis sizes of dihedral and Boolean groups. We find a lower bound for the basis size of a Boolean group. We also calculate basis sizes for dihedral and Boolean groups of small orders.

1 Introduction

A subset B of a group G is called a *basis* of G if each element $g \in G$ can be written as g = ab for some $a, b \in B$. The smallest cardinality of a basis of G is called the *basis size* of G and is denoted by r[G]. The problem of estimating r[G] for a cyclic group G was first proposed by Schur and various bounds were obtained by Rohrbach [13], Moser [10], Stöhr [15], Klotz [7] and others. Bases for arbitrary groups were dealt by Rohrbach [14] and lately by Cherly [5], Bertram and Herzog [4], Nathanson [11], Kozma and Lev [8].

A family \mathcal{G} of finite groups is *well-based* if there exists a constant $c \in \mathbb{R}_+$ such that $r[G] \leq c\sqrt{|G|}$ for each $G \in \mathcal{G}$. Bertram and Herzog [4] showed that the families of nilpotent groups, as well as the families of the alternating and symmetric groups, are well-based. Kozma and Lev [8] proved (using the classification of finite simple groups) that $r[G] \leq \frac{4}{\sqrt{3}}\sqrt{|G|}$ for any finite group G. Therefore, the family of all finite groups is well-based.

The definition of a basis B for a group G implies that $|G| \leq |B|^2$, and hence $r[G] \geq \sqrt{|G|}$. The fraction

$$\delta[G] := \frac{r[G]}{\sqrt{|G|}} \ge 1$$

is called the *basis characteristic* of G.

In this paper we shall evaluate basis characteristics of dihedral and Boolean groups. We recall that the *dihedral group* D_{2n} of order 2n is the isometry group of a regular *n*-gon. The dihedral group D_{2n} contains a normal cyclic subgroup of index 2. A standard model of a cyclic group of order *n* is the multiplicative group

$$C_n = \{ z \in \mathbb{C} : z^n = 1 \}$$

of *n*-th roots of 1. The group C_n is isomorphic to the additive group of the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. A group *G* is called *Boolean* if $g^{-1} = g$ for every $g \in G$. It is well-known that Boolean groups are Abelian and are isomorphic to the powers of the two-element cyclic group C_2 .

Kozma and Lev [8] proved that each finite group G has the basis characteristic $\delta[G] \leq \frac{4}{\sqrt{3}} \approx 2.3094$. Until now, the best estimate for an upper bound of the basis characteristic was the estimate for the class of cyclic groups: each cyclic group C_n has the basis characteristic $\delta[C_n] \leq 2$. We shall show that for dihedral groups this upper bound can be improved to $\delta[D_{2n}] \leq \frac{24}{\sqrt{146}} \approx 1.9862$. Moreover, if $n \geq 2 \cdot 10^{15}$, then $\delta[D_{2n}] < \frac{4}{\sqrt{6}} \approx 1.633$. Also we prove that each Boolean group G has the basis size $\frac{1+\sqrt{8|G|-7}}{2} \leq r[G] < \frac{3}{\sqrt{2}}\sqrt{|G|}$ and, therefore, its basis characteristic $\delta[G] < \frac{3}{\sqrt{2}} \approx 2.1213$.

For a class \mathcal{G} of finite groups the number

$$\delta[\mathcal{G}] = \sup_{G \in \mathcal{G}} \delta[G]$$

is called the *basis characteristic* of the class \mathcal{G} .

For a real number x we put

$$\lceil x \rceil = \min\{n \in \mathbb{Z} : n \ge x\} \text{ and } \lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \le x\}.$$

2 Known results

In this section we recall some known results on bases in finite groups. Kozma and Lev [8] proved the following fundamental fact.

Theorem 1. Each finite group G has the basis characteristic $\delta[G] \leq \frac{4}{\sqrt{3}}$.

Bertram and Herzog [4] proved the following proposition.

Proposition 2. Let G be a finite group. Then

- 1) $r[G] \leq |G:H| \cdot r[H]$ for any subgroup $H \subset G$;
- 2) $r[G] \leq r[G/H] \cdot |H|$ for any normal subgroup $H \subset G$;
- 3) $r[G] \leq 2r[G/H] \cdot r[H]$ for any normal subgroup $H \subset G$;

4) $r[G] \leq |H| + |G:H| - 1$ for any subgroup $H \subset G$.

In evaluating basis characteristics of dihedral groups we shall use difference characteristics of cyclic groups. A subset B of a group G is called a *difference basis* of G if each element $g \in G$ can be written as $g = xy^{-1}$ for some $x, y \in B$. The smallest cardinality of a difference basis of G is called the *difference size* of G and is denoted by $\Delta[G]$. The definition of a difference basis B for a group G implies that $|G| \leq |B|^2$, and hence $\Delta[G] \geq \sqrt{|G|}$. The fraction

$$\eth[G] := \frac{\Delta[G]}{\sqrt{|G|}} \ge 1$$

is called the *difference characteristic* of G.

Difference basis have applications in the study of structure of superextensions of groups, see [1, 3].

Difference sizes of finite cyclic groups were evaluated in [2] with the help of difference sizes of the order-intervals $[1, n] \cap \mathbb{Z}$ in the additive group \mathbb{Z} of integer numbers. For a natural number $n \in \mathbb{N}$ by $\Delta[n]$ we shall denote the difference size of the order-interval $[1, n] \cap \mathbb{Z}$ and by $\eth[n] := \frac{\Delta[n]}{\sqrt{n}}$ its difference characteristic. The asymptotics of the sequence $(\eth[n])_{n=1}^{\infty}$ was studied by Rédei and Rényi [12], Leech [9] and Golay [6] who eventually proved that

$$\sqrt{2 + \frac{4}{3\pi}} < \sqrt{2 + \max_{0 < \varphi < 2\pi} \frac{2\sin(\varphi)}{\varphi + \pi}} \le \lim_{n \to \infty} \eth[n] = \inf_{n \in \mathbb{N}} \eth[n] \le \eth[6166] = \frac{128}{\sqrt{6166}} < \eth[6] = \sqrt{\frac{8}{3}}.$$

Banakh and Gavrylkiv [2] applied difference sizes of the order-intervals $[1, n] \cap \mathbb{Z}$ to give upper bounds for difference sizes of finite cyclic groups.

Proposition 3. For every $n \in \mathbb{N}$ the cyclic group C_n has the difference size $\Delta[C_n] \leq \Delta[\lceil \frac{n-1}{2} \rceil]$, which implies that

$$\limsup_{n \to \infty} \eth[C_n] \le \frac{1}{\sqrt{2}} \inf_{n \in \mathbb{N}} \eth[n] \le \frac{64}{\sqrt{3083}} < \frac{2}{\sqrt{3}}.$$

Banakh and Gavrylkiv [2] proved the following upper bound for difference characteristics of cyclic groups.

Theorem 4. For any $n \in \mathbb{N}$ the cyclic group C_n has the difference characteristic:

- 1) $\eth[C_n] \leq \eth[C_4] = \frac{3}{2};$
- 2) $\eth[C_n] \leq \eth[C_2] = \eth[C_8] = \sqrt{2}$ if $n \neq 4$;

3)
$$\eth[C_n] \le \frac{12}{\sqrt{73}} < \sqrt{2} \text{ if } n \ge 9;$$

- 4) $\eth[C_n] \leq \frac{24}{\sqrt{293}} < \frac{12}{\sqrt{73}}$ if $n \geq 9$ and $n \neq 292$;
- 5) $\eth[C_n] < \frac{2}{\sqrt{3}}$ if $n \ge 2 \cdot 10^{15}$.

The following Table 1 of difference sizes and characteristics of cyclic groups C_n for ≤ 100 is taken from [2].

n	$\Delta[C_n]$	$\eth[C_n]$	n	$\Delta[C_n]$	$\eth[C_n]$	n	$\Delta[C_n]$	$\eth[C_n]$	n	$\Delta[C_n]$	$\eth[C_n]$
1	1	1	26	6	1.1766	51	8	1.1202	76	10	1.1470
2	2	1.4142	27	6	1.1547	52	9	1.2480	77	10	1.1396
3	2	1.1547	28	6	1.1338	53	9	1.2362	78	10	1.1322
4	3	1.5	29	7	1.2998	54	9	1.2247	79	10	1.1250
5	3	1.3416	30	7	1.2780	55	9	1.2135	80	11	1.2298
6	3	1.2247	31	6	1.0776	56	9	1.2026	81	11	1.2222
7	3	1.1338	32	7	1.2374	57	8	1.0596	82	11	1.2147
8	4	1.4142	33	7	1.2185	58	9	1.1817	83	11	1.2074
9	4	1.3333	34	7	1.2004	59	9	1.1717	84	11	1.2001
10	4	1.2649	35	7	1.1832	60	9	1.1618	85	11	1.1931
11	4	1.2060	36	7	1.1666	61	9	1.1523	86	11	1.1861
12	4	1.1547	37	7	1.1507	62	9	1.1430	87	11	1.1793
13	4	1.1094	38	8	1.2977	63	9	1.1338	88	11	1.1726
14	5	1.3363	39	7	1.1208	64	9	1.125	89	11	1.1659
15	5	1.2909	40	8	1.2649	65	9	1.1163	90	11	1.1595
16	5	1.25	41	8	1.2493	66	10	1.2309	91	10	1.0482
17	5	1.2126	42	8	1.2344	67	10	1.2216	92	11	1.1468
18	5	1.1785	43	8	1.2199	68	10	1.2126	93	12	1.2443
19	5	1.1470	44	8	1.2060	69	10	1.2038	94	12	1.2377
20	6	1.3416	45	8	1.1925	70	10	1.1952	95	12	1.2311
21	5	1.0910	46	8	1.1795	71	10	1.1867	96	12	1.2247
22	6	1.2792	47	8	1.1669	72	10	1.1785	97	12	1.2184
23	6	1.2510	48	8	1.1547	73	9	1.0533	98	12	1.2121
24	6	1.2247	49	8	1.1428	74	10	1.1624	99	12	1.2060
25	6	1.2	50	8	1.1313	75	10	1.1547	100	12	1.2

Table 1: Difference sizes and characteristics of cyclic groups C_n for $n \leq 100$.

3 Basis sizes and characteristics of dihedral groups

In this section we shall evaluate basis sizes and characteristics of dihedral groups. The following proposition yields some upper bounds for the basis size of a dihedral group.

Proposition 5. For any numbers $n, m \in \mathbb{N}$ the dihedral group D_{2nm} has the basis size

- 1) $r[D_{2nm}] \le 2n \cdot r[C_m];$
- 2) $r[D_{2nm}] \leq r[D_{2n}] \cdot m;$
- 3) $r[D_{2nm}] \le 2r[D_{2n}] \cdot r[C_m].$

Proof. It is well-known that the dihedral group D_{2nm} contains a normal cyclic subgroup of order nm, which can be identified with the cyclic group C_{nm} . The subgroup $C_m \subset C_{nm}$ is normal in D_{2mn} and the quotient group D_{2mn}/C_m is isomorphic to D_{2n} . Applying Proposition 2(1-3), we obtain the desired upper bounds.

Theorem 6. For any $n \in \mathbb{N}$ the dihedral group D_{2n} has the basis size $r[D_{2n}] \leq 2\Delta[C_n]$.

Proof. It is well-known that the group D_{2n} contains a cyclic subgroup C_n and an element $s \in D_{2n} \setminus C_n$ such that $s = s^{-1}$ and $sxs = x^{-1}$ for all $x \in C_n$. Fix a difference basis $B \subset C_n$ of cardinality $|B| = \Delta[C_n]$. Therefore, $BB^{-1} = C_n$ and $sBs = B^{-1}$. We claim that $B^{-1} \cup sB$ is a basis. Indeed,

$$(B^{-1} \cup sB)(B^{-1} \cup sB) = B^{-1}B^{-1} \cup B^{-1}sB \cup sBB^{-1} \cup sBsB \supset s(BB^{-1}) \cup (sBs)B$$
$$= sC_n \cup B^{-1}B = (D_{2n} \setminus C_n) \cup BB^{-1} = (D_{2n} \setminus C_n) \cup C_n = D_{2n}.$$
Therefore, $r[D_{2n}] \le |B^{-1} \cup sB| = 2|B| = 2\Delta[C_n].$

In Table 2 we present the results of computer calculations of basis sizes and characteristics of dihedral groups of order ≤ 80 .

2n	$r[D_{2n}]$	$2\Delta[C_n]$	$\delta[D_{2n}]$	2n	$r[D_{2n}]$	$2\Delta[C_n]$	$\delta[D_{2n}]$
2	2	2	1.4142	42	9	10	1.3887
4	3	4	1.5	44	9	12	1.3568
6	3	4	1.2247	46	9	12	1.3269
8	4	6	1.4142	48	9	12	1.2990
10	4	6	1.2649	50	9	12	1.2727
12	5	6	1.4433	52	10	12	1.3867
14	5	6	1.3363	54	10	12	1.3608
16	5	8	1.25	56	10	12	1.3363
18	6	8	1.4142	58	10	14	1.3130
20	6	8	1.3416	60	10	14	1.2909
22	7	8	1.4924	62	10	12	1.2700
24	6	8	1.2247	64	11	14	1.375
26	7	8	1.3728	66	10	14	1.2309
28	7	10	1.3228	68	11	14	1.3339
30	7	10	1.2780	70	10	14	1.1952
32	7	10	1.2374	72	11	14	1.2963
34	8	10	1.3719	74	11	14	1.2787
36	8	10	1.3333	76	12	16	1.3764
38	8	10	1.2977	78	11	14	1.2455
40	8	12	1.2649	80	12	16	1.3416

Table 2: Basis sizes and characteristics of dihedral groups D_{2n} for $2n \leq 80$.

Theorem 7. Let D_{2n} be a dihedral group of order 2n. Then for any number $n \in \mathbb{N}$, the basis characteristic of the dihedral group is $\delta[D_{2n}] \leq \frac{24}{\sqrt{146}}$. If $n \geq 2 \cdot 10^{15}$, then $\delta[D_{2n}] < \frac{4}{\sqrt{6}}$.

Proof. It is well-known that the dihedral group D_{2n} contains a normal cyclic subgroup of order n, which can be identified with the cyclic group C_n . Applying Theorem 6, we obtain the upper bound

$$\delta[D_{2n}] = \frac{r[D_{2n}]}{\sqrt{2n}} \le \frac{2\Delta[C_n]}{\sqrt{2n}} = \sqrt{2} \cdot \eth[C_n].$$

If $n \ge 9$, then using part 3 of Theorem 4, we get $\eth[C_n] \le \frac{12}{\sqrt{73}}$. Therefore,

$$\delta[D_{2n}] \le \sqrt{2} \cdot \frac{12}{\sqrt{73}} = \frac{24}{\sqrt{146}}$$

Analyzing the data from Table 2, one can check that $\delta[D_{2n}] \leq \frac{24}{\sqrt{146}} \approx 1.9863$ for all $n \leq 8$.

If $n \ge 2 \cdot 10^{15}$, then using part 5 of Theorem 4, we get $\eth[C_n] < \frac{2}{\sqrt{3}}$, and hence

$$\delta[D_{2n}] \le \sqrt{2} \cdot \eth[C_n] < \frac{4}{\sqrt{6}}.$$

r			
L			
L			

The results of computer calculations given in Table 2 and Theorem 7 imply the following lower and upper bounds for the basis characteristic of the class Dihedral of dihedral groups.

Proposition 8. The class Dihedral of dihedral groups has the basis characteristic

$$1.5 = \frac{3}{\sqrt{4}} = \delta[D_4] \le \delta[\mathsf{Dihedral}] \le \frac{24}{\sqrt{146}} \approx 1.9863.$$

Proof. Theorem 7 yields the upper bound

$$\delta[\mathsf{Dihedral}] = \sup_{n \in \mathbb{N}} \delta[D_{2n}] \le \frac{24}{\sqrt{146}}.$$

On the other hand, the basis size $r[D_4] = 3$ of the dihedral group D_4 witnesses that

$$1.5 = \delta[D_4] \le \delta[\mathsf{Dihedral}].$$

Question 9. Is $\delta[\text{Dihedral}] = \delta[D_4] = 1.5?$

4 Basis sizes and characteristics of Boolean groups

In this section we evaluate basis sizes and characteristics of finite Boolean groups. A group G is called *Boolean* if $g^{-1} = g$ for every $g \in G$. It is well-known that Boolean groups are Abelian and are isomorphic to the powers of the two-element cyclic group C_2 . Let Boolean denote the class of finite Boolean groups and let Boolean₀ := { $G \in \text{Boolean} : \sqrt{|G|} \in \mathbb{N}$ }.

We start with the lower bound for r[G].

Theorem 10. Each Boolean group G has $r[G] \ge \frac{1+\sqrt{8|G|-7}}{2}$.

Proof. Take a basis $B \subset G$ of cardinality |B| = r[G] and consider the surjective map $\xi : B \times B \to G, \xi : (x, y) \mapsto xy$. Observe that for the unit e of the group G the preimage $\xi^{-1}(e)$ coincides with the diagonal $\{(x, y) \in B \times B : x = y\}$ of the square $B \times B$, and hence has cardinality $|\xi^{-1}(e)| = |B|$. Observe also that for any element $g \in G \setminus \{e\}$ and any $(x, y) \in \xi^{-1}(g)$, we get $x \neq y$ and yx = xy = g, which implies that $|\xi^{-1}(g)| \ge 2$. Then

$$|B|^{2} = |B \times B| = |\xi^{-1}(e)| + \sum_{g \in G \setminus \{e\}} |\xi^{-1}(g)| \ge |B| + 2(|G| - 1).$$

Therefore, $|B|^2 - |B| - 2(|G| - 1) \ge 0$, and hence $r[G] = |B| \ge \frac{1 + \sqrt{1 + 8(|G| - 1)}}{2} = \frac{1 + \sqrt{8|G| - 7}}{2}$. **Theorem 11.** Each finite Boolean group G has

$$\frac{1+\sqrt{8|G|-7}}{2} \le r[G] < \begin{cases} 2\sqrt{|G|}, & \text{if } G \in \mathsf{Boolean}_0; \\ \frac{3}{\sqrt{2}}\sqrt{|G|}, & \text{otherwise.} \end{cases}$$

Proof. The lower bound $\frac{1+\sqrt{8|G|-7}}{2} \leq r[G]$ follows from Theorem 10.

The group G, being Boolean, is isomorphic to $(C_2)^n$ for some $n \ge 0$. Let $k = \lfloor \frac{n}{2} \rfloor$ and find a subgroup $H \subset G$ of order 2^k . By Proposition 2(4), $r[G] \le |H| + |G/H| - 1$.

If $G \in \mathsf{Boolean}_0$, then n = 2k is even and

$$r[G] \le |H| + |G/H| - 1 = 2^k + 2^k - 1 < 2\sqrt{2^{2k}} = 2\sqrt{|G|}.$$

If $G \notin \mathsf{Boolean}_0$, then n = 2k + 1 is odd and

$$r[G] \le |H| + |G/H| - 1 = 2^k + 2^{k+1} - 1 < \frac{3}{\sqrt{2}}\sqrt{2^{2k+1}} = \frac{3}{\sqrt{2}}\sqrt{|G|}.$$

In the following Table 3 we present the results of computer calculations of basis sizes and characteristics of Boolean groups $(C_2)^n$ for $n \leq 6$. In this table

$$lb[G] := \left\lceil \frac{1 + \sqrt{8|G| - 7}}{2} \right\rceil$$
 and $ub[G] := \left\lfloor \sqrt{\frac{9|G|}{2}} \right\rfloor$

are the lower and upper bounds given in Theorems 10 and 11.

Theorem 11 implies the following corollaries.

G	C_2	$(C_2)^2$	$(C_2)^3$	$(C_2)^4$	$(C_2)^5$	$(C_2)^6$
lb[G]	2	3	5	6	9	12
r[G]	2	3	5	6	10	14
ub[G]	3	4	6	8	12	16
$\delta[G]$	1.4142	1.5	1.7677	1.5	1.7677	1.75

Table 3: Basis sizes and characteristics of Boolean groups $(C_2)^n$ for $n \leq 6$.

Corollary 12. The class Boolean of finite Boolean groups has the basis characteristic

$$1.7677... = \frac{5}{\sqrt{8}} = \delta[(C_2)^3] \le \delta[\text{Boolean}] \le \frac{3}{\sqrt{2}} = 2.1213..$$

Proof. The upper bound $\delta[\text{Boolean}] \leq \frac{3}{\sqrt{2}}$ follows from Theorem 11 and the lower bound $\delta[\text{Boolean}] \geq \delta[(C_2)^3] = \frac{5}{\sqrt{8}}$ follows from the known value $r[(C_2)^3] = 5$.

Corollary 13. The class $Boolean_0$ has the basis characteristic

$$1.75 = \frac{14}{\sqrt{64}} = \delta[(C_2)^6] \le \delta[\text{Boolean}_0] \le 2$$

Proof. The upper bound $\delta[\mathsf{Boolean}_0] \leq 2$ follows from Theorem 11 and the lower bound $\delta[\mathsf{Boolean}_0] \geq \delta[(C_2)^6] = 1.75$ follows from the known value $r[(C_2)^6] = 14$.

References

- T. Banakh and V. Gavrylkiv, Algebra in the superextensions of twinic groups, *Disserta*tiones Math. 473 (2010), 3–74.
- T. Banakh and V. Gavrylkiv, Difference bases in cyclic groups, preprint, 2017, https://arxiv.org/abs/1702.02631.
- [3] T. Banakh, V. Gavrylkiv, and O. Nykyforchyn, Algebra in superextension of groups, I: zeros and commutativity, *Algebra Discrete Math.* **3** (2008), 1–29.
- [4] E. A. Bertram and M. Herzog, On medium-size subgroups and bases of finite groups, J. Combin. Theory Ser. A 57 (1991), 1–14.
- [5] J. Cherly, On complementary sets of group elements, Arch. Math. 35 (1980), 313–318.
- [6] M. Golay, Notes on the representation of 1, $2, \ldots, n$ by differences, J. London Math. Soc. 4 (1972) 729–734.
- [7] W. Klotz, Eine obere Schranke f
 ür die Reichweite einer Extremalbasis zweiter Ordnung, J. Reine Angew. Math. 238 (1969), 161–168.

- [8] G. Kozma and A. Lev, Bases and decomposition numbers of finite groups, Arch. Math. (Basel) 58 (1992), 417–424.
- [9] J. Leech, On the representation of $1, 2, \ldots, n$ by differences, J. London Math. Soc. **31** (1956), 160–169.
- [10] L. Moser, On the representation of $1, 2, \ldots, n$ by sums, Acta Arith. 6 (1960), 11–13.
- [11] M. B. Nathanson, On a problem of Rohrbach for finite groups, J. Number Theory 41 (1992), 69–76.
- [12] L. Rédei and A. Rényi, On the representation of the numbers 1, 2, ..., N by means of differences, Mat. Sbornik N.S. 24 (1949), 385–389.
- [13] H. Rohrbach, Ein Beitrag zur additiven Zahlentheorie, Math. Z. 42 (1937), 1–30.
- [14] H. Rohrbach, Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretische Frage, Math. Z. 42 (1937), 538–542.
- [15] A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe, I, J. Reine Angew. Math. 194 (1955), 40–65.

2010 Mathematics Subject Classification: Primary 05B10; Secondary 05E15, 20D60. Keywords: dihedral group, Boolean group, basis, basis size, basis characteristic.

Received April 18 2017; revised versions received April 20 2017; June 24 2017; June 26 2017; July 6 2017. Published in *Journal of Integer Sequences*, July 31 2017.

Return to Journal of Integer Sequences home page.