Norms and Distances over Finite Groups

Vladimir Batagelj *
University of Ljubljana, Department of Mathematics
Jadranska 19, 61 111 Ljubljana, Yugoslavia

Current version: October 21, 1990

Abstract

In the paper norms and distances over finite groups are studied. A characterization of ultrametric interval group norms is given. It is proved that the maximal range of interval group norms is attained on groups which are the powers of the cyclic group of order two.

Key words : finite groups, interval group norms, distances, ordered partitions, Hamming norm, (generalized) Lee norm, Sharma-Kaushik partitions.

Math. Subj. Class. (1985) : 20 D 60, 54 E 35, 11 T 71, 94 B 60

During professor Sharma's presentation of his paper *Association and other Schemes Related to Sharma-Kaushik Class of Distances over Finite Rings* [2] we noticed that in the construction of a distance, using the weight induced by a partition, we need only the structure of the group $(\mathbb{Z}_q, +_q)$. The idea of the construction can be extended to any (finite) group provided that the weight is a 'group norm'. We were convinced that group norms would already have been studied; but it took us several days to finally find a reference on this subject [8]. Another reference [3] was pointed out by one of the referees. The proposition 5 was the only result that we did not know before reading [8]. Although some basic facts about group norms can also be found in [8], we decided to reproduce them to make our paper easier to read.

1 Group norms

Let $(A, \bullet, e)$ be a finite group with a neutral element e. We denote the inverse element of $a \in A$ by a'. The mapping $w : A \to \mathbb{R}$ is a *(group) norm* if it has the following properties:

*Supported in part by the Research Council of Slovenia, Yugoslavia; and by the Yugoslav Federal Grant P-339.

E. $\forall a \in A : (w(a) = 0 \Leftrightarrow a = e)$

S. $\forall a \in A : w(a) = w(a')$

and

N. $\forall a, b \in A : (w(a) + w(b) \geq w(a \bullet b))$

If the mapping w has the properties E, S and

U. $\forall a, b \in A : (\max(w(a), w(b)) \geq w(a \bullet b))$

we shall call it an *ultrametric (group) norm* [4, p. 39]. We shall denote the normed group by $(A, \bullet, e; w)$.

Several proofs for ultrametric norms are essentially the same as for ordinary norms. In these cases we shall use the symbol $\oplus$ to denote the operation max or addition.

Let us list some properties of group norms:

Proposition 1 *For all* $a \in A : w(a) \geq 0$.

Proposition 2 *Every ultrametric group norm is also a group norm.*

From group theory we know that the product $(A \times B, \star, e)$ of two groups $(A, \bullet, e_A)$ and $(B, \circ, e_B)$, where

$$(a, b) \star (\alpha, \beta) = (a \bullet \alpha, b \circ \beta)$$

is also a group. The following proposition shows that we can extend norms from groups to their products.

Proposition 3 *Let* $(A, \bullet, e_A; u)$ *and* $(B, \circ, e_B; v)$ *be (ultrametric) normed groups. Then the group* $(A \times B, \star, e; w)$ *is also a (ultrametric) normed group, for the norm*

$$w(a, b) = u(a) \oplus v(b)$$

Remark: Because every ultrametric norm is a norm we can also combine by addition ultrametric norms, obtaining an ordinary norm. ∎

Given a normed group $(A, \bullet, e, w)$ we can define a mapping $d : A \times A \to \mathbb{R}$ by the equality

$$d(a, b) = w(a \bullet b')$$

The mapping d has several interesting properties:

Proposition 4 *Let* $G = (A, \bullet, e; w)$ *be a normed group and let* $d(a, b) = w(a \bullet b')$ *then for all* $a, b, c \in A$ *it holds:*

D1. $d(a, b) = 0 \Leftrightarrow a = b$

D2. $d(a, b) = d(b, a)$

D3. $d(a, b) \oplus d(b, c) \geq d(a, c)$

D4. $d(a \bullet c, b \bullet c) = d(a, b)$

and if the group G *is Abelian*

D5. $d(a, b') = d(a', b)$

D6. $d(a, b) = d(a', b')$

The first three properties D1, D2 and D3 say that d is a *distance*, which is by D4 *invariant under right translations.*

Proposition 5 *(Ultrametric) group norms determine exactly the (ultrametric) distances invariant under right translations.*

2 Constructions of group norms

In this section we shall deal with the problem how to define a norm on a finite group.

Let A be a finite set. Any symmetric function $d : A \times A \to \mathbb{R}$ with zero diagonal can be transformed into a distance by

$$\delta(a,b) = \begin{cases} 0 & a = b \\ d(a,b) + \Delta & a \neq b \end{cases}$$

where Δ is a constant greater than $\max_{a,b,c \in A}(d(a,c) - d(a,b) - d(b,c))$.

Therefore it is obvious that there exist distances over a group $(A, \bullet, e)$ which are not invariant under right translations. For example, the distance d determined by the table

d	0	1	2	3
0	0	1	1	1
1	1	0	1	1
2	1	1	0	2
3	1	1	2	0

is not invariant under right translations over $(\mathbb{Z}_4, +_4, 0)$:

$$d(0,1) = 1 \neq 2 = d(2,3) = d(0 +_4 2, 1 +_4 2)$$

For these reasons, to be able to exploit the properties of the underlying groups, we shall limit our discussion in the following to distances induced by group norms.

To define a group norm over a finite group some well known results can be used.

In a finite group G the order of an element has the properties $\mathrm{ord}(e) = 1$ and $\mathrm{ord}(a') = \mathrm{ord}(a)$. If the group is Abelian it also holds

$$\mathrm{ord}(a \bullet b) \leq \mathrm{ord}(a) \cdot \mathrm{ord}(b)$$

Therefore:

Proposition 6 *Let $G = (A, \bullet, e)$ be a finite Abelian group. Then*

$$w(a) = \log \mathrm{ord}(a)$$

is a group norm.

Each finite group is finitely generated. Therefore, given a finite set of generators, we can define $w(a)$ as the length of the shortest word (composed of generators and their inverses) which equals to the element a.

It is easy to prove:

Proposition 7 *Let $G = (A, \bullet)$ and $H = (B, \circ)$ be groups and $\varphi : A \to B$ a monomorphism and w a group norm on H. Then the function $v : A \to \mathbb{R}$ defined by*

$$v(a) = w(\varphi(a))$$

is also a group norm on G.

Some classical results from coding theory can be extended to finite groups or expressed in terms of group norms:

Proposition 8 *Let $G = (A, \bullet)$ be a finite group. Then the function $h : A \to \mathbb{N}$ defined by*

$$h(a) = \begin{cases} 0 & a = e \\ 1 & a \neq e \end{cases}$$

is an ultrametric group norm; called the Hamming norm.

Therefore on every finite group we can define at least one ultrametric group norm. Are there any others ?

Proposition 9 *Let $(\mathbb{Z}_n, +_n)$ be a cyclic group on n elements. Then the function $l : \mathbb{Z}_n \to \mathbb{N}$ defined by*

$$l(a) = \min(a, n - a)$$

is a group norm; called the Lee norm.

Hamming and Lee norms induce a partition of the set $\mathbb{Z}_q$ – each class consists of elements which have equal value of the norm. This observation was used by Sharma and Kaushik [1, 2] in the construction of Sharma-Kaushik class of partitions/distances on $\mathbb{Z}_q$; but it can be generalized further.

Let $(A, \bullet, e)$ be a finite group and $\Pi = \{\pi(0), \pi(1), \ldots, \pi(k)\}$, $\pi(0) = \{e\}$ an *ordered partition* of the set A. Then we can define a weight

$$w(a) = i \Leftrightarrow a \in \pi(i)$$

The weight w has the property $w(A) = \{0, 1, \ldots k\}$. A group norm w with this property we shall call an *interval norm* . To each interval norm w corresponds an ordered partition

$$\pi(i) = \{a \in A : w(a) = i\}$$

Hamming and Lee norms are special cases of interval norms.

What are the conditions on the ordered partition Π that give us a group norm w ?

The first condition is evident: for each element $a \in A$ both a and a' belong to the same class π from Π:

$$\forall a \in A : (a \in \pi \Rightarrow a' \in \pi)$$

For the second condition, let us define

$$\sigma(k) = \bigcup_{i=0}^{k} \pi(i)$$

Therefore

$$\pi(k) = \sigma(k) \setminus \sigma(k-1)$$

The ordered partition Π induces an interval group norm iff besides the first condition it also satisfies

$$a \in \sigma(i) \wedge b \in \sigma(j) \Rightarrow a \bullet b \in \sigma(i + j)$$

or for ultrametric interval group norm

$$a, b \in \sigma(i) \Rightarrow a \bullet b \in \sigma(i)$$

In the case of an ultrametric interval group norm the second condition requires that $\sigma(i)$ is a stable subset of the finite group – a subgroup. We obtain

Proposition 10 *Let $G = (A, \bullet, e)$ be a finite group. Then the partition Π induces an ultrametric group norm iff the corresponding sets $\sigma(i)$ form a nested sequence of subgroups of G.*

In the applications of interval norms in coding theory the following their property can be useful.

Proposition 11 *Let $(A, \bullet, e; w)$ be a finite group with an interval norm w. Then for every $a \in A$ and $t \in w(A)$ there exists an element $b \in A$ such that $d(a, b) = t$.*

Proof: From the definition of distance d it follows

$$\{d(a, b) : b \in A\} = \{w(a \bullet b') : b \in A\} =$$

and because $\{a \bullet b' : b \in A\} = A$ we have

$$= \{w(b) : b \in A\} = w(A)$$

■

A *(generalized) Lee norm* is an interval norm for which each class has a form $\pi(i) = \{a, a'\}$. Does a Lee norm exist for each finite group ?

Proposition 12 *Let $G = (A, \bullet, e_A; u)$ and $H = (B, \circ, e_B; v)$ be finite groups with interval norms u and v. Then their direct product $G \times H = (A \times B, \star, e; w)$ is also a group with interval norm defined by*

$$w((a, b)) = u(a) + (m + 1).v(b)$$

where $m = \max_{a \in A} u(a)$.

Proof:

E. $0 = w((a, b)) = u(a) + (m + 1).v(b) \Leftrightarrow$
$u(a) = 0 \wedge v(b) = 0 \Leftrightarrow a = e_A \wedge b = e_B$

S. $w((a, b)') = w((a', b')) = u(a') + (m + 1).v(b') =$
$u(a) + (m + 1).v(b) = w((a, b))$

N. $w((a, b)) + w((c, d)) =$
$(u(a) + (m + 1).v(b)) + (u(c) + (m + 1).v(d)) =$
$(u(a) + u(c)) + (m + 1)(v(b) + v(d)) \geq$
$u(a \bullet c) + (m + 1)v(b \circ d) = w((a \bullet c, b \circ d)) = w((a, c) \star (b, d))$

■

For a finite group $G = (A, \bullet)$, let $N(G)$ denote the maximal value of all interval group norms over G ; and let

$$p = |\{a \in A : a' \neq a\}| \qquad \text{and} \qquad s = |\{a \in A : a^2 = e\}|$$

We have $p + s = n = |A|$ and $1 \leq s \leq n$. From the definition of interval norms it follows

$$N(G) \leq s + \frac{p}{2} - 1 = n - 1 - \frac{1}{2}(n - s)$$

The equality holds iff there exists a Lee norm over G. Therefore

$$N(\mathcal{C}_n) = \left\lfloor \frac{n}{2} \right\rfloor$$

Let

$$N(n) = \max_{|G|=n} N(G)$$

It is evident that:

$$\left\lfloor \frac{n}{2} \right\rfloor \leq N(n) \leq n - 1$$

If n is a prime number then $N(n) = \lfloor \frac{n}{2} \rfloor$. The only group of this order is $\mathcal{C}_n$.

Proposition 13 *$N(n) = n - 1$ iff $n = 2^k$. This bound is obtained uniquely on the group $\mathcal{C}_2^k$.*

Proof: If $n = 2^k$ by proposition 12 it follows $N(\mathcal{C}_2^k) = n - 1$.

If $N(n) = n - 1$ then there exists a group G of order n which has in its Cayley table all diagonal elements equal e. Therefore in G we have for all $a \in A : a^2 = e$. This implies [5, p. 100] that $G = \mathcal{C}_2^k$. ■

3 Examples

By computer inspection of small groups we obtained the results presented in Table 1. The contents of its columns are the following:

group	– name of the group;
n	– order of the group;
$\#\Pi$	– number of ordered partitions, $\pi(0) = \{e\},\ a, a' \in \pi$;
$\#w$	– number of interval norms;
w_{max}	– range of maximal interval norm;
$\#w_{max}$	– number of maximal interval norms;
$\#u$	– number of ultrametric interval norms;
u_{max}	– range of maximal ultrametric interval norm;
$\#\bar{\Pi}$	– number of bad partitions.

For the quaternion group (its Cayley table is given on the left part of Table 2) we obtained 3 maximal ultrametric interval norms

Table 1: Interval group norms on small groups

group	n	$\#\Pi$	$\#w$	w_{max}	$\#w_{max}$	$\#u$	u_{max}	$\#\bar{\Pi}$
$\mathcal{C}_2$	2	1	1	1	1	1	1	0
$\mathcal{C}_3$	3	1	1	1	1	1	1	0
$\mathcal{C}_4$	4	3	3	2	2	2	2	0
$\mathcal{C}_2^2$	4	13	13	3	6	4	2	0
$\mathcal{C}_5$	5	3	3	2	2	1	1	0
$\mathcal{C}_6$	6	13	12	3	5	3	2	0
$\mathcal{S}_3$	6	75	48	4	6	5	2	0
$\mathcal{C}_7$	7	13	10	3	3	1	1	0
$\mathcal{C}_8$	8	75	40	4	8	4	3	0
$\mathcal{C}_4 \times \mathcal{C}_2$	8	541	222	5	28	12	3	0
$\mathcal{C}_2^3$	8	47293	5622	7	168	36	3	63
$\mathcal{D}_4$	8	4683	920	6	40	16	3	9
$\mathcal{Q}$	8	75	48	4	12	8	3	0
$\mathcal{C}_9$	9	75	33	4	3	2	2	0
$\mathcal{C}_{10}$	10	541	136	5	10	3	2	0
$\mathcal{D}_5$	10	47293	2364	7	20	7	2	156
$\mathcal{C}_{11}$	11	541	96	5	5	1	1	0
$\mathcal{C}_{12}$	12	4683	545	6	14	8	3	20
$\mathcal{D}_6$	12	7087261	55193	9	60	34	3	7432

e	E	i	I	j	J	k	K
0	1	2	2	3	3	3	3
0	1	3	3	2	2	3	3
0	1	3	3	3	3	2	2

and 12 maximal interval norms

e	E	i	I	j	J	k	K
0	1	2	2	3	3	4	4
0	1	2	2	4	4	3	3
0	1	3	3	2	2	4	4
0	1	3	3	4	4	2	2
0	1	4	4	2	2	3	3
0	1	4	4	3	3	2	2

e	E	i	I	j	J	k	K
0	2	1	1	3	3	4	4
0	2	1	1	4	4	3	3
0	2	3	3	1	1	4	4
0	2	3	3	4	4	1	1
0	2	4	4	1	1	3	3
0	2	4	4	3	3	1	1

For the dihedral group $\mathcal{D}_4$ (its Cayley table is given on the right part of Table 2) we list only the 7 maximal ultrametric interval norms

Table 2: Quaternion group $\mathcal{Q}$ and dihedral group $\mathcal{D}_4$

$*$	e	E	i	I	j	J	k	K
e	e	E	i	I	j	J	k	K
E	E	e	I	i	J	j	K	k
i	i	I	E	e	k	K	J	j
I	I	i	e	E	K	k	j	J
j	j	J	K	k	E	e	i	I
J	J	j	k	K	e	E	I	i
k	k	K	j	J	I	i	E	e
K	K	k	J	j	i	I	e	E
x'	e	E	I	i	J	j	K	k

$*$	e	a	b	c	E	A	B	C
e	e	a	b	c	E	A	B	C
a	a	b	c	e	A	B	C	E
b	b	c	e	a	B	C	E	A
c	c	e	a	b	C	E	A	B
E	E	C	B	A	e	c	b	a
A	A	E	C	B	a	e	c	b
B	B	A	E	C	b	a	e	c
C	C	B	A	E	c	b	a	e
x'	e	c	b	a	E	A	B	C

e	a	b	c	E	A	B	C
0	2	1	2	3	3	3	3
0	3	1	3	2	3	2	3
0	3	1	3	3	2	3	2
0	3	2	3	1	3	2	3
0	3	2	3	2	3	1	3
0	3	2	3	3	1	3	2
0	3	2	3	3	2	3	1

and 9 bad partitions – partitions which can not be ordered in a way giving an interval norm.

$$\{\{e\},\{ac\},\{bE\},\{A\},\{BC\}\}$$
$$\{\{e\},\{ac\},\{bE\},\{AB\},\{C\}\}$$
$$\{\{e\},\{ac\},\{bA\},\{E\},\{BC\}\}$$
$$\{\{e\},\{ac\},\{bA\},\{EC\},\{B\}\}$$
$$\{\{e\},\{ac\},\{bB\},\{EA\},\{C\}\}$$
$$\{\{e\},\{ac\},\{bB\},\{EC\},\{A\}\}$$
$$\{\{e\},\{ac\},\{bC\},\{E\},\{AB\}\}$$
$$\{\{e\},\{ac\},\{bC\},\{EA\},\{B\}\}$$
$$\{\{e\},\{acb\},\{E\},\{A\},\{B\},\{C\}\}$$

Conclusion

In this paper we have presented some ideas and results on norms over finite groups. Several problems remain open.

We conjectured that for every finite group a Lee norm exists. Recently Bojan Mohar and Martin Juvan proved that no Lee norm exists for A_4 and that a Lee norm exists for every dihedral group D_n. Therefore:

$$N(\mathcal{D}_n) = n + \left\lfloor \frac{n}{2} \right\rfloor$$

The basic results of coding theory [7, 6] can be directly extended to codes over finite groups. Let $G = (A, \bullet, e; w)$ be a finite group with an interval norm and $C \subseteq A$ a *code*. We define the *error-order* of $a \in A$ by

$$\varepsilon(a) = \min_{c \in C} d(c, a)$$

and the *minimum distance* by

$$\delta(C) = \min\{d(a, b) : a, b \in C,\ a \neq b\}$$

For example, it is easy to prove that:

Proposition 14 *A code C can correct by nearest neighbour decoding all the errors of order up to t if*

a. $\delta(C) \geq 2t + 1$, *d is a distance;*

or

b. $\delta(C) > t$, *d is an ultrametric distance.*

The converse of this proposition does not hold. The following simple counterexample was given by one of the referees.

Let $G = (\{0, a, b, c\}, +)$ denote the Klein four group $\mathcal{C}_2^2$: $x + x = 0$ all x, $a + b = c$, $a + c = b$, $b + c = a$. Define

$$w(0) = 0, \quad w(a) = 1, \quad w(b) = 2, \quad w(c) = 3.$$

One easily checks that this is an interval norm. Let $C = \{0, b\}$. Then $\delta(C) = 2$. However, the code C can correct all errors of order up to 1.

References

[1] Bhu Dev Sharma, Manohar Lal Kaushik (1986), "Algebra of Sharma and Kaushik's Metric Inducing Partitions of $\mathbb{Z}_q$". *Journal of Combinatorics, Information & System Sciences*, **11**, 19-32.

[2] Bhu Dev Sharma, Norris Sooko, (1989), "Association and other Schemes Related to Sharma-Kaushik Class of Distances over Finite Rings". *Paper presented at the II. Catania Combinatorial Conference, Santa-Tecla, September 1989.*

[3] Clark W.E., Gur Dial, "Remarks on the Sharma-Kaushik Metrics for Error-correcting Codes". To appear in JCISS.

[4] Dieudonné J.(1969), *Foundations of Modern Analysis*. Academic Press, New York.

[5] Gilbert W.J. (1976), *Modern Algebra with Applications*. Wiley, New York.

[6] Hill R. (1986), *A First Course in Coding Theory*. Clarendon Press, Oxford.

[7] Stone H.S. (1973), *Discrete Mathematical Structures and their Applications*. SRA, Chicago.

[8] Zamansky M. (1963), *Introduction a l'algèbre et l'analyse modernes*. Dunod, Paris.