ADDITIVE NUMBER THEORY SHEDS EXTRA LIGHT ON THE HOPF-STIEFEL o FUNCTION

L'Enseignement Mathématique, t. 49 (2003), p. 109–116

ADDITIVE NUMBER THEORY SHEDS EXTRA LIGHT ON THE HOPF-STIEFEL ○ FUNCTION

by Alain PLAGNE

ABSTRACT. The famous Hopf-Stiefel ○ function appears in several places in mathematics (linear and bilinear algebra, topology, intercalate matrices, ...). However, although the object of much study, this function kept a part of mystery since no simple formula was known for it. We shall derive a simple and practical explicit formula for ○ and more generally for β_p (p arbitrary prime), a generalized function due to Eliahou and Kervaire. The proof relies on a new result in combinatorial group theory which follows from additive number theoretical arguments. It is shown that this last result generalizes earlier ones by Eliahou and Kervaire and by Yuzvinsky.

1. INTRODUCTION

A *composition formula* of size $[r, s, n]$ over some field $\mathbf{F}$ (that we assume to be of characteristic different from 2) is an identity of the form

$$(x_1^2 + \cdots + x_r^2)(y_1^2 + \cdots + y_s^2) = (z_1^2 + \cdots + z_n^2)\,,$$

where $z_1, z_2, \ldots, z_n$ are n bilinear forms in the variables $(x_1, \ldots, x_r)$ and $(y_1, \ldots, y_s)$, with coefficients in $\mathbf{F}$. For example, the law of moduli for complex numbers provides the identity

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_2y_1 + x_1y_2)^2\,,$$

which is a composition formula of size $[2, 2, 2]$. The law of moduli for quaternions (respectively for octonions) provides a composition formula of size $[4, 4, 4]$ (respectively $[8, 8, 8]$) in a similar way. Conversely, Hurwitz's theorem [7] (see also [8]) states that the only possible values of n for which a composition formula of size $[n, n, n]$ exists are $1, 2, 4$ and 8.

In the late thirties, starting from the Hurwitz problem, Hopf [6] and Stiefel [15] began to study real division algebras. They introduced a function of an algebraic nature. The so-called Hopf-Stiefel function $\circ$ (which depends on two positive integral variables r and s) is defined by the formula

$$r \circ s = \min\{n \text{ such that } (x+y)^n = 0 \text{ in } \mathbf{F}_2[x,y]/(x^r, y^s)\}. \tag{1.1}$$

Hopf and Stiefel obtained a result which says that if a nonsingular bilinear map from $\mathbf{R}^r \times \mathbf{R}^s$ onto $\mathbf{R}^n$ exists over $\mathbf{R}$, then $n \geq r \circ s$ (Hopf-Stiefel theorem). The link between nonsingular bilinear maps and $\circ$ is realized by passing to projective spaces and their cohomology rings.

More generally, the $\circ$ function appears in different parts of mathematics. It allows a nice mathematical trip: starting from bilinear algebra (Hurwitz's problem, Pfister's quadratic forms [10, 11]) and algebra (its basic definition (1.1)), we pass through topology (Hopf-Stiefel theorem, real division algebras and Yuzvinsky's theorem [17]), visit the theory of intercalate matrices (Yuzvinsky's conjecture [17, 16]) and arrive at additive number theory ([5] and the present paper). The reader interested in the many applications of $\circ$ is mainly referred to the nice survey [13] by Shapiro, to his recent book [14, Chapters 12-15] and to the book by Rajwade [12], especially Chapter 13.

With the algebraic viewpoint (1.1), it is fairly natural to generalize, with Eliahou and Kervaire [5], the $\circ$ function in the following way. For any given prime p, we set

$$\beta_p(r,s) = \min\{n \text{ such that } (x+y)^n = 0 \text{ in } \mathbf{F}_p[x,y]/(x^r, y^s)\}.$$

Evidently, $\beta_2 = \circ$. It is a theorem of Eliahou and Kervaire [5] that this extension of (1.1) is still relevant in the additive number theoretical context.

Although many properties of $\circ$ and more generally of β_p were known (for instance recursion formulas or expression in terms of p-adic expansions), describing these functions efficiently appeared difficult, so that it is not rare to see tables giving the first values of $\circ$.

In this paper, perhaps surprisingly, we shall derive a simple and practical explicit formula for $\circ$ and more generally for β_p (p arbitrary prime).

THEOREM 1. *Let p be any prime number. The function β_p is given by the formula*

$$\beta_p(r,s) = \min_{t \in \mathbf{N}} \left(\lceil r/p^t \rceil + \lceil s/p^t \rceil - 1 \right) p^t .$$

Notice that clearly, the minimum involved is attained for a value of t satisfying $0 \leq t \leq \lceil \log(\max(r,s))/\log p \rceil$.

In particular, this result elucidates, in some sense, the Hopf-Stiefel function.

THEOREM 2. *The Hopf-Stiefel function is*

$$r \circ s = \min_{t \in \mathbf{N}} \left(\lceil r/2^t \rceil + \lceil s/2^t \rceil - 1 \right) 2^t .$$

With this formula, a large number of properties of $\circ$ follow immediately or admit a simplified proof.

In fact Theorem 1 follows from an additive number theoretical theorem (Theorem 3 below) which is of independent interest. Given a finite Abelian group G, we define (as in [5]) the function of two integral variables r and s $(1 \leq r, s \leq |G|)$

$$\mu_G(r,s) = \min\{|\mathcal{A} + \mathcal{B}|, \text{ with } \mathcal{A}, \mathcal{B} \subset G, \ |\mathcal{A}| = r, \ |\mathcal{B}| = s\}$$

where $\mathcal{A} + \mathcal{B}$ is the usual Minkowski sum of sets, namely

$$\mathcal{A} + \mathcal{B} = \{a + b \text{ with } a \in \mathcal{A}, \ b \in \mathcal{B}\} .$$

Given an arbitrary Abelian group G, determining the function μ_G is not easy: this is an open problem in general for G finite and Abelian. However, Eliahou and Kervaire [5] obtained such a result for finite groups of prime exponent, thus generalizing Yuzvinsky's result [17] for binary spaces.

Using a different approach (based on Kneser's theorem [9]), we shall obtain a result valid for any *cyclic* group.

THEOREM 3. *Let n be any integer. If $1 \leq r, s \leq n$, we have*

$$\mu_{\mathbf{Z}/n\mathbf{Z}}(r,s) = \min_{d|n} \left(\lceil r/d \rceil + \lceil s/d \rceil - 1 \right) d .$$

Taking $n = p$, a prime, gives exactly the Cauchy-Davenport theorem [2, 3, 4]. Moreover, as will be explained in Section 3, this result contains that of Eliahou and Kervaire.

Since cyclic groups are characterized by the equality $\exp G = |G|$, this theorem is a direct consequence of the following more general result.

THEOREM 4. *Let G be any finite Abelian group. Then, if $1 \leq r, s \leq |G|$, we have*

$$\min_{d \,||G|} \left(\lceil r/d \rceil + \lceil s/d \rceil - 1 \right) d \leq \mu_G(r,s) \leq \min_{\frac{|G|}{\exp G} \,|\, d \,||G|} \left(\lceil r/d \rceil + \lceil s/d \rceil - 1 \right) d .$$

With these results, we know the behaviour of μ_G at the two endpoints of the spectrum (cyclic groups and groups of prime exponent). What now remains to be done is to fill the gap between the upper bound and the lower bound for general finite Abelian groups.

2. Proof of Theorem 4

Let G be any given finite Abelian group and let $1 \leq r, s \leq |G|$.

2.1 The lower bound

If $\mu_G(r,s) \geq r+s-1$, the result is immediate (take $d=1$). We may thus assume that

$$\mu_G(r,s) \leq r+s-1\,. \tag{2.1}$$

Then, choosing two sets $\mathcal{A}$ and $\mathcal{B}$ in G with respective cardinalities r and s, such that $|\mathcal{A}+\mathcal{B}|$ attains $\mu_G(r,s)$, we get

$$|\mathcal{A}+\mathcal{B}| = \mu_G(r,s) \leq |\mathcal{A}|+|\mathcal{B}|-1\,.$$

We are in a position to apply Kneser's theorem [9] on the structure of sets with a small sumset. It follows that there exists a subgroup H of G (namely the stabilizer of $\mathcal{A}+\mathcal{B}$) such that

$$|\mathcal{A}+\mathcal{B}| = |\mathcal{A}+H|+|\mathcal{B}+H|-|H|\,.$$

Denoting by $(\mathcal{A}+H)/H$ (resp. $(\mathcal{B}+H)/H$) the H-cosets that $\mathcal{A}$ (resp. $\mathcal{B}$) intersects, we obtain

$$\begin{aligned} |\mathcal{A}+\mathcal{B}| &= \left(\left|\frac{\mathcal{A}+H}{H}\right|+\left|\frac{\mathcal{B}+H}{H}\right|-1\right)|H| \\ &\geq (\lceil r/f\rceil+\lceil s/f\rceil-1)f \end{aligned}$$

where f denotes the cardinality of H. Since Lagrange's theorem shows that f divides $|G|$, we get

$$|\mathcal{A}+\mathcal{B}| \geq \min_{d\,|\,|G|}(\lceil r/d\rceil+\lceil s/d\rceil-1)d\,.$$

From this it follows that, in any case,

$$\mu_G(r,s) \geq \min_{d\,|\,|G|}(\lceil r/d\rceil+\lceil s/d\rceil-1)d\,,$$

which is the desired lower bound.

2.2 THE UPPER BOUND

Let H be any subgroup of G. Choose $\mathcal{A}_0$ and $\mathcal{B}_0$ in G/H with respective cardinalities $\lceil r/|H| \rceil$ and $\lceil s/|H| \rceil$ and such that

$$|\mathcal{A}_0 + \mathcal{B}_0| = \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil) .$$

Now choose $\mathcal{A}$ of cardinality r and $\mathcal{B}$ of cardinality s in G such that the image of $\mathcal{A}$ (resp. $\mathcal{B}$) by the canonical projection on G/H is included in $\mathcal{A}_0$ (resp. $\mathcal{B}_0$). One has

$$|\mathcal{A} + \mathcal{B}| \leq \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil)|H| .$$

This proves the first lemma we need.

LEMMA 1. *For any finite Abelian group* G

$$\mu_G(r, s) \leq \min_{H \leq G} \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil)|H| .$$

The second useful point is synthesized in the next folkloric lemma.

LEMMA 2. *Let* G *be a finite Abelian group. For any positive integer* m, *the following two propositions are equivalent*

(i) m *divides* $\exp G$,

(ii) *there exists a subgroup* H *of* G *such that* G/H *is isomorphic to* $\mathbf{Z}/m\mathbf{Z}$.

In the case of a *cyclic* group K, trivial considerations (take two sets with consecutive elements), show that, for any $u, v \leq |K|$,

$$\mu_K(r, s) \leq r + s - 1 . \tag{2.2}$$

Using consecutively Lemma 1, inequality (2.2) and Lemma 2 yields the following chain of inequalities:

$$\begin{aligned}
\mu_G(r, s) &\leq \min_{H \leq G} \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil)|H| \\
&\leq \min_{H \leq G,\ G/H \text{ cyclic}} \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil)|H| \\
&\leq \min_{H \leq G,\ G/H \text{ cyclic}} \left(\lceil r/|H| \rceil + \lceil s/|H| \rceil - 1\right)|H| \\
&= \min_{|G/H| \text{ divides } \exp G} \left(\lceil r/|H| \rceil + \lceil s/|H| \rceil - 1\right)|H| \\
&= \min_{f | \exp G} \left(\lceil rf/|G| \rceil + \lceil sf/|G| \rceil - 1\right) \frac{|G|}{f} .
\end{aligned}$$

The change of variable $d = |G|/f$ yields a parameter d subject to the two restrictions $\frac{|G|}{\exp G} \mid d$ and $d \mid |G|$; this proves the upper bound in Theorem 4.

3. From Theorem 3 to Theorem 1

We first use the theorem of Eliahou and Kervaire (see Section 3 of [5]), which states that if p is an arbitrary prime, r and s two integers, then

$$\beta_p(r,s) = \mu_{(\mathbf{Z}/p\mathbf{Z})^d}(r,s) \tag{3.1}$$

whenever $p^d \geq r, s$.

Now, from Theorem 10 of [1], it follows that μ_G coincides with $\mu_{G'}$ as soon as G and G' are two Abelian p-groups of the same order. In other words,

$$\mu_{(\mathbf{Z}/p\mathbf{Z})^d}(r,s) = \mu_{\mathbf{Z}/p^d\mathbf{Z}}(r,s)\,. \tag{3.2}$$

We would like to emphasize that from our method (more precisely, using simply Lemma 1) together with an inductive argument (the quotient groups of $(\mathbf{Z}/p\mathbf{Z})^d$ have the same form), we are able to derive a simple direct (that is, without using [1]) alternative proof of (3.2). Indeed, the only thing to verify is that if

$$r+s-1 < \left(\lceil r/p^k\rceil + \lceil s/p^k\rceil - 1\right)p^k \tag{3.3}$$

for any $k \geq 1$ then we can construct sets $\mathcal{A}$ and $\mathcal{B}$ of respective cardinalities r and s with $|\mathcal{A}+\mathcal{B}| = r+s-1$. This is achieved by taking for $\mathcal{A}$ (resp. for $\mathcal{B}$) the r (resp. the s) smallest possible elements in the sense of the lexicographic order. Hypothesis (3.3) then ensures that, in this case, $|\mathcal{A}+\mathcal{B}| = r+s-1$.

We are now ready to prove Theorem 1. We put for instance $d = r+s$ (but any sufficiently large d will do). Using consecutively (3.1), (3.2) and Theorem 3, we obtain

$$\begin{aligned}
\beta_p(r,s) &= \mu_{(\mathbf{Z}/p\mathbf{Z})^d}(r,s)\\
&= \mu_{\mathbf{Z}/p^d\mathbf{Z}}(r,s)\\
&= \min_{t|p^d}\left(\lceil r/t\rceil + \lceil s/t\rceil - 1\right)t\\
&= \min_{u\leq d}\left(\lceil r/p^u\rceil + \lceil s/p^u\rceil - 1\right)p^u\\
&= \min_{u\in\mathbf{N}}\left(\lceil r/p^u\rceil + \lceil s/p^u\rceil - 1\right)p^u,
\end{aligned}$$

which proves Theorem 3.

ACKNOWLEDGEMENTS. I was introduced to the μ function by Shalom Eliahou during the conference "Multilinear Algebra and Matroid Theory" held in Lisboa, Portugal (March 24–26, 2002). There, he asked me for a formula for $\mu_{\mathbf{Z}/n\mathbf{Z}}$, a question which led me to Theorem 3. He then kindly indicated to me the application to the β_p functions. The author is grateful to Shalom Eliahou for his help as well as for a careful reading of preliminary versions of this paper. I would like to associate Michel Kervaire to these thanks, for the interest he took in this paper.

REFERENCES

[1] BOLLOBAS, B. and I. LEADER. Sums in the grid. *Discrete Math. 162* (1996), 31–48.

[2] CAUCHY, A.L. Recherches sur les nombres. *J. École polytechnique* (1813), 99–123.

[3] DAVENPORT, H. On the addition of residue classes. *J. London Math. Soc. 10* (1935), 30–32.

[4] —— A historical note. *J. London Math. Soc. 22* (1947), 100–101.

[5] ELIAHOU, S. and M. KERVAIRE. Sumsets in vector spaces over finite fields. *J. Number Theory 71* (1998), 12–39.

[6] HOPF, H. Ein topologischer Beitrag zur reellen Algebra. *Comment. Math. Helv. 13* (1940–41), 219–239.

[7] HURWITZ, A. Über die Komposition der quadratischen Formen von beliebig vielen Variabeln. *Nachr. Ges. Wiss. Göttingen* (1898), 309–316.

[8] —— Über die Komposition der quadratischen Formen. *Math. Ann. 88* (1923), 1–25.

[9] KNESER, M. Abschätzung der asymptotischen Dichte von Summenmengen. *Math. Z. 58* (1953), 459–484.

[10] PFISTER, A. Zur Darstellung von -1 als Summe von Quadraten in einem Körper. *J. London Math. Soc. 40* (1965), 159–165.

[11] —— Quadratische Formen in beliebigen Körpern. *Invent. Math. 1* (1966), 116–132.

[12] RAJWADE, A.R. *Squares.* LMS Lecture Notes *171*. Cambridge, 1993.

[13] SHAPIRO, D. Products of sums of squares. *Exposition. Math. 2* (1984), 235–261.

[14] —— *Compositions of Quadratic Forms.* Walter de Gruyter, Berlin, 2000.

[15] STIEFEL, E. Über Richtungsfelder in den projektiven Räumen und einen Satz aus der reellen Algebra. *Comment. Math. Helv. 13* (1940–41), 201–218.

[16] YIU, P. On the product of two sums of 16 squares as a sum of squares of integral bilinear forms. *Quart. J. Math. Oxford Ser. (2) 41* (1990), 463–500.

[17] YUZVINSKY, S. Orthogonal pairings of Euclidean spaces. *Michigan Math. J.* *28* (1981), 109–119.

(Reçu le 6 décembre 2002)

Alain Plagne

LIX
École polytechnique
F-91128 Palaiseau Cedex
France
e-mail: plagne@lix.polytechnique.fr