Astérisque

AST

Structure theory of set addition - Pages préliminaires

Astérisque, tome 258 (1999), p. I-XXII

<http://www.numdam.org/item?id=AST_1999__258__R1_0>

ASTÉRISQUE 258

STRUCTURE THEORY OF SET ADDITION

edited by
Jean-Marc Deshouillers
Bernard Landreau
Alexander A. Yudin

Société Mathématique de France 1999

Jean-Marc Deshouillers
Mathématiques stochastiques, Université Bordeaux 2, BP 26,
33076 Bordeaux, France.
E-mail : j-m.deshouillers@u-bordeaux2.fr

Bernard Landreau
Laboratoire A2X, Université Bordeaux 1, 33405 Talence Cedex, France.
E-mail : landreau@math.u-bordeaux.fr

Alexander A. Yudin
Department of Mathematics, Vladimir Pedagogical University,
11, pr. Stroiteley, Vladimir, Russia.
E-mail : aayudin@vgpu.elcom.ru

1991 ***Mathematics Subject Classification.*** — 05-XX, 11Bxx, 11Hxx, 11Lxx, 11Pxx, 20Cxx, 20Dxx, 20Exx, 20Fxx, 60Exx, 60Fxx, 68Qxx, 90Cxx, 94Bxx.

Key words and phrases. — additive number theory, combinatorial number theory, additive finite groups, structure theory of set addition, inverse additive problems, sums of discrete random variables, subset sums, integer programming, coding theory.

STRUCTURE THEORY OF SET ADDITION

edited by Jean-Marc Deshouillers, Bernard Landreau, Alexander A. Yudin

Abstract. — For a long time, additive number theory, motivated by conjectures such as that of Goldbach or Waring, has been concerned by the study of additive properties of *special* sequences. In the 1930's it was noticed that the consideration of the additive properties of *general* sequences turned out, not only to be a beautiful subject for its own sake, but was able to lead to improvements in the study of special sequences: thus, in the paper founding this philosophy, Schnirel'man introduced a density on sets of integers, gave a general lower bound for the density of the sum of two sets, and applied it to the special sequence of primes to show that every integer can be written as a sum of a uniformly bounded number of primes. Additive number theory evolved towards the definition of invariants for sets of (non-necessarily commutative) monoids and the study of the invariants for the "sum" of different sets in terms of the invariants of those sets.

A new trend appeared in the 1950's, with authors like M. Kneser and G. A. Freiman, which is sometimes described as *inverse* additive theory: knowing that the relation between the invariants of a family of sets and the invariant of their sum is extremal (or close to), what can be said on the *structure* of the sets themselves ?

In the recent years, there has been a renewed interest for this approach which turns out to have applications to different others fields. It seemed appropriate to gather in a single volume 24 contemporary original research papers and 3 survey articles dealing with *the structure theory of set addition* and its applications to elementary or combinatorial number theory, group theory, integer programming and probability theory.

Résumé **(Problèmes additifs inverses).** — La théorie additive des nombres, motivée par des conjectures telles que celles de Goldbach ou Waring, s'est longtemps consacrée à l'étude des propriétés additives de suites *particulières*. Dans les années 1930, on a remarqué que la considération des propriétés additives de suites *générales*, non seulement constituait un magnifique sujet en lui-même, mais en outre permettait des améliorations dans l'étude de suites particulières : ainsi, dans l'article fondateur de cette problématique, Schnirel'man a introduit une notion de densité sur les suites d'entiers, donné une minoration de la densité de la somme de deux suites et l'a appliquée à l'ensemble des nombres premiers montrant que tout entier peut être

représenté comme une somme de nombres premiers, avec un nombre de termes uniformément borné. La théorie additive des nombres a évolué vers la définition d'invariants pour des parties de monoïdes (non nécessairement commutatifs) et l'étude des invariants de la somme d'ensembles en fonction des invariants liés à ces ensembles.

Une nouvelle tendance est apparue dans les années 1950, avec les travaux de M. Kneser et G.A. Freiman, que l'on désigne parfois sous le vocable de théorie additive *inverse* : sachant que le rapport entre les invariants d'une famille d'ensembles et l'invariant de leur somme est extrêmal (ou presque extrêmal), que peut-on dire de la *structure* des ensembles eux-mêmes ?

Cet abord a connu récemment un regain d'intérêt qui se trouve porter ses fruits dans d'autres domaines. Il a semblé judicieux de regrouper en un unique volume 24 articles de recherches originaux et 3 synthèses ayant trait à cette théorie de la structure des sommes d'ensembles et ses applications à la théorie des nombres élémentaire ou combinatoire, à la théorie des groupes, à la programmation entière et à la théorie des probabilités.

Contents

Combinatorial Number Theory

Algebra

Coding Theory

Integer Programming

Probability

RÉSUMÉS DES ARTICLES

Nous présentons une synthèse des résultats fondamentaux de la théorie connue sous le nom de "structure theory of set addition" et de leurs applications à d'autres domaines.

Nous cherchons à optimiser, pour un entier k et un réel u fixés, sur tous les ensembles $K = \{a_1 < a_2 < \cdots < a_k\} \subset \mathbb{Z}$, la mesure de l'ensemble des $\alpha \in [0,1]$ tels que la valeur absolue de la somme trigonométrique $S_K(\alpha) = \sum_{j=1}^{k} e^{2\pi i \alpha a_j}$ soit supérieure à $k - u$. Lorsque u est suffisamment petit par rapport à k, nous sommes en mesure de construire un ensemble K_{ex} qui est presque optimal. Cet ensemble est une union finie de progressions arithmétiques. Nous montrons que tout ensemble plus performant, s'il existe, a une structure similaire à celle de K_{ex}. On obtient également des bornes inférieures et supérieures précises pour la mesure maximale.

Freiman a démontré qu'un ensemble fini d'entiers K satisfaisant $|K+K| \leq \sigma|K|$ est nécessairement un sous-ensemble d'une petite progression arithmétique généralisée de rang m avec $m \leq \lfloor \sigma - 1 \rfloor$. Nous donnons une preuve complète de ce résultat accompagnée de quelques améliorations ainsi que du calcul explicite des constantes impliquées.

Si un ensemble fini A d'entiers inclus dans $\{1, \ldots, N\}$ a plus de N/k éléments, on peut s'attendre à ce que l'ensemble ℓA des sommes de ℓ éléments de

application, on prouve que $|T| \geq 2k-3$ sous ces conditions. Des résultats antérieurs de Freiman jouent un rôle essentiel dans les démonstrations.

On the number of sums and differences

Dans cet article, nous montrons que $\inf_{A\subset\mathbb{Z}} \ln|A+A|/\ln|A-A|$ est inférieur à 0,7865, améliorant en cela un résultat antérieur dû à G. Freiman et W. Pigarev.

The structure of multisets with a small number of subset sums

On recherche ici des ensembles d'entiers naturels $A = \{a_1, \ldots, a_k\}$ (avec répétitions possibles) tels que l'ensemble des sommes $P(A) = \{\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k : 0 \leq \varepsilon_1, \ldots, \varepsilon_k \leq 1\}$ est petit. Précisément, soit A un tel ensemble pour lequel le cardinal de $P(A)$ est borné par un multiple fixe du cardinal de A (i.e. $|P(A)| \ll |A|$), nous montrons que l'ensemble $P(A)$ est alors la réunion d'un petit nombre de progressions arithmétiques de même raison.

Des problèmes similaires ont déjà été considérés par G. Freiman [1] et M. Chaimovich [2]. À la différence de ces articles, nos conditions s'expriment seulement à l'aide du cardinal de $P(A)$ sans faire appel au plus grand élément de A.

Subset sums of sets of residues

On appelle nombre critique d'un groupe abélien G, le plus petit entier naturel m vérifiant la propriété suivante :
pour toute partie A de G avec $|A| \geq m, 0 \notin A$, l'ensemble A^* des sommes partielles de A est égal à G. Dans cet article, on démontre la conjecture de G. Diderrich concernant la valeur du nombre critique du groupe G, lorsque $G = \mathbb{Z}_q$, pour q suffisamment grand.

Inverse theorems and the number of sums and products

Soit $\epsilon > 0$. Erdős et Szemerédi ont conjecturé que, si A est un ensemble de k nombres entiers positifs avec k assez grand, le nombre des entiers qui sont représentables comme somme ou produit de deux éléments de A est au moins égal à $k^{2-\epsilon}$. Nous confirmons cette conjecture dans le cas particulier où le nombre des sommes est très petit.

Stratified Sets

On dit qu'un ensemble $\mathcal{A}$ de nombres entiers est "stratifié" si, pour tout t, $0 \leq t < \operatorname{Card}\mathcal{A}$, la somme de t éléments distincts de $\mathcal{A}$ est toujours strictement inférieure à la somme de $t+1$ éléments distincts de $\mathcal{A}$. Cela implique que les

éléments de $\mathcal{A}$ sont positifs. On démontre que le nombre d'ensembles stratifiés de plus grand élément N est exactement égal au nombre $p(N)$ de partitions de N.

On the structure of sets of lattice points in the plane with a small doubling property

On décrit la structure des ensembles $\mathbb{K}$ de points d'un réseau plan tels que $|\mathbb{K}+\mathbb{K}|$ est petit comparé à $|\mathbb{K}|$. Soit $\mathbb{K}$ un sous-ensemble fini de $\mathbb{Z}^2$ tel que

$$|\mathbb{K}+\mathbb{K}| < 3.5|\mathbb{K}| - 7.$$

Si $\mathbb{K}$ est porté par trois droites parallèles, alors l'enveloppe convexe de $\mathbb{K}$ est contenu dans trois progressions arithmétiques compatibles de même raison ayant en totalité au plus

$$|\mathbb{K}| + \frac{3}{4}\Big(|\mathbb{K}+\mathbb{K}| - \frac{10}{3}|\mathbb{K}| + 5\Big)$$

termes. Cette majoration est optimale.

Non-solvable groups with a large fraction of involutions

Dans cet article, on classifie les groupes finis G non résolubles tels que le nombre de classes de G est au moins $|G|/16$. On en déduit certaines conséquences.

Questions on set squaring in groups

Quelques questions sur des petits sous-ensembles de groupes sont posées et discutées.

On groups generated by a pair of elements with small third or fourth power

Cet article se propose d'étudier les groupes bi-générés, tels que la puissance m-ème de la paire génératrice contienne moins de $2m$ éléments. Nous prouvons en particulier, que si le cube de la paire génératrice contient moins de 7 éléments ou si la puissance quatrième contient moins de 11 éléments, alors le groupe est résoluble. Sinon, il n'est pas nécessairement résoluble. Les démonstrations sont effectuées à l'aide de calculs par ordinateurs.

On small subset product in a group

Nous généralisons des théorèmes d'addition connus pour le cas des groupes non abéliens.

Les preuves classiques des théorèmes d'addition utilisent des transformations locales dues à Davenport, Dyson et Kempermann.

Notre approche est basée sur l'étude de certains blocs d'imprimitivité du groupe d'automorphismes d'une relation.

New results on subset multiplication in groups
MARCEL HERZOG 309

Cet article présente des résultats et des problèmes ouverts sur les sujets suivants : groupes avec sous-tables de multiplication déficientes, bases multiplicatives des groupes finis.

On small sumsets in abelian groups
VSEVOLOD F. LEV 317

On étudie dans cet article la structure des paires de parties finies A, B d'un groupe abélien pour lesquelles les sommes sont peu nombreuses : $|A + B| < |A| + |B|$. En 1960, J. H. B. Kemperman en a donné une description complète de nature récursive mais relativement compliquée. En utilisant des résultats intermédiaires de Kemperman, on obtient ici une description d'une autre nature. Bien qu'elle ne soit pas suffisante d'un point de vue général, notre description a l'avantage d'être claire et intuitive, et peut être utilisée pour des applications.

An analog of Freiman's theorem in groups
IMRE Z. RUZSA 323

On montre que pour un groupe abélien G, tel que l'ordre des éléments est majoré par un entier r, tout ensemble ayant n éléments et au plus αn sommes est contenu dans un sous-groupe de taille Cn avec $C = f(r, \alpha)$ dépendant de r et α mais non de n. C'est un résultat analogue au Théorème de G. Freiman qui décrit la sructure de tels ensembles dans le groupe des entiers.

Subset sums and coding theory
GÉRARD COHEN & GILLES ZÉMOR 327

Nous nous intéressons à quelques problèmes additifs dans le groupe $(\mathbb{Z}/2\mathbb{Z})^r$. Notre propos est de montrer comment ces problèmes sont étroitement liés à la théorie des codes correcteurs. Nous présentons des techniques classiques de codage que nous utilisons pour obtenir quelques contributions originales.

New Structural Approach to Integer Programming: a Survey
MARK CHAIMOVICH 341

Cet article de synthèse présente un nouvel abord de la programmation entière basée sur la caractérisation de configurations extrêmes en théorie additive des nombres. La structure de ces configurations extrêmes nous permet d'élaborer des algorithmes applicables à des familles suffisamment larges de problèmes; ces algorithmes améliorent notablement les bornes actuellement connues. Là où ils sont applicables, ces algorithmes sont polynômiaux voire linéaires; c'est en particulier le cas pour les problèmes de type sac à dos. Pour

cette classe de problèmes, l'amélioration sur les algorithmes antérieurs est d'au moins de deux ordres de grandeur.

New Algorithm for Dense Subset-Sum Problem

On présente un nouvel algorithme pour le problème des sommes partielles (subset-sum problem) dans le cas dense. Il est basé sur une caractérisation de la famille des sommes partielles obtenue par des méthodes analytiques de la théorie additive des nombres. L'algorithme fonctionne pour un grand nombre de sommants (m) avec des valeurs qui sont majorées. La borne (ℓ) dépend modérément de m. Le temps requis par ce nouvel algorithme est en $O(m^{7/4}/\log^{3/4} m)$, ce qui est plus rapide que les précédents algorithmes connus, le meilleur d'entre eux prenant un temps en $O(m^2/\log^2 m)$.

On the Two-Dimensional Subset Sum Problem

Dans cet article, on considère un système de deux équations booléennes linéaires. Grâce à des méthodes de théorie analytique des nombres, on montre que, sous certaines conditions, le système admet toujours des solutions. Cela complète le travail de Freiman sur ce sujet.

On series of discrete random variables, 1: real trinomial distributions with fixed probabilities

Cet article démarre l'étude du comportement limite local d'un système triangulaire de variables aléatoires indépendantes $(\zeta_{n,k})_{1\leq k\leq n}$, où la loi de $\zeta_{n,k}$ dépend de n. Nous considédrons le cas où $\zeta_{n,1}$ prend trois valeurs entières $0 < a_1(n) < a_2(n)$ avec des probabilités respectives p_0, p_1, p_2 qui ne dépendent pas de n. Nous montrons qu'il y a trois types de comportement limite pour la suite des variables aléatoires $\eta_n = \zeta_{n,1} + \cdots + \zeta_{n,n}$, selon que $a_2(n)/\mathrm{pgcd}(a_1(n), a_2(n))$ tend vers l'infini plus lentement, plus vite ou à la même vitesse que $\sqrt{n}$.

On Bounds for the Concentration Function. 1

Nous donnons une majoration de la fonction de concentration d'une somme de variables aléatoires entières indépendantes et équidistribuées, en fonction d'une minoration de leur queue de distribution, sous l'hypothèse supplémentaire nécessaire que le support de ces variables aléatoires n'est pas essentiellement contenu dans une progression arithmétique non triviale.

ABSTRACTS

We review fundamental results in the so-called structure theory of set addition as well as their applications to other fields.

We investigate the problem of optimizing, for a fixed integer k and real u and on all sets $K = \{a_1 < a_2 < \cdots < a_k\} \subset \mathbb{Z}$, the measure of the set of $\alpha \in [0,1]$ where the absolute value of the trigonometric sum $S_K(\alpha) = \sum_{j=1}^{k} e^{2\pi i \alpha a_j}$ is greater than $k-u$. When u is sufficiently small with respect to k we are able to construct a set K_{ex} which is very close to optimal. This set is a union of a finite number of arithmetic progressions. We are able to show that any more optimal set, if one exists, has a similar structure to that of K_{ex}. We also get tight upper and lower bounds on the maximal measure.

Freiman proved that a finite set of integers K satisfying $|K+K| \leq \sigma|K|$ is a subset of a "small" m-dimensional arithmetical progression, where $m \leq \lfloor \sigma - 1 \rfloor$. We give a complete self-contained exposition of this result, together with some refinements, and explicitly compute the constants involved.

If a finite set A of integers included in $\{1,\ldots,N\}$ has more than N/k elements, one may expect that the set ℓA of sums of ℓ elements of A, contains, when ℓ is comparable to k, a rather long arithmetic progression (which can be required to be homogeneous or not). After presenting the state of the art, we show that some of the results cannot be improved as far as it would be thought possible in view of the known results in the infinite case. The paper ends with

We investigate multisets of natural numbers with relatively few subset sums. Namely, let A be a multiset such that the number of distinct subset sums of A is bounded by a fixed multiple of the cardinality of A (that is, $|P(A)| \ll |A|$). We show that the set $P(A)$ of subset sums is then a union of a small number of arithmetic progressions sharing a common difference.

Similar problems were considered by G. Freiman (see [1]) and M. Chaimovich (see [2]). Unlike those papers, our conditions are stated in terms of the cardinality of the subset sums set $P(A)$ only and not on the largest element of the original multiset A.

The result obtained is nearly best possible.

The number m is called the critical number of a finite abelian group G, if it is the minimal natural number with the property:
for every subset A of G with $|A| \geq m, 0 \notin A$, the set of subset sums A^* of A is equal to G. In this paper, we prove the conjecture of G. Diderrich about the value of the critical number of the group G, in the case $G = \mathbb{Z}_q$, for sufficiently large q.

Let $\epsilon > 0$. Erdős and Szemerédi conjectured that if A is a set of k positive integers which large k, there must be at least $k^{2-\epsilon}$ integers that can be written as the sum or product of two elements of A. We shall prove this conjecture in the special case that the number of sums is very small.

A set $\mathcal{A}$ of integers is said "stratified" if, for all t, $0 \leq t < \operatorname{Card} \mathcal{A}$, the sum of any t distinct elements of $\mathcal{A}$ is smaller than the sum of any $t+1$ distinct elements of $\mathcal{A}$. That implies that all elements of $\mathcal{A}$ should be positive. It is proved that the number of stratified sets with maximal element equal to N is exactly the number $p(N)$ of partitions of N.

We describe the structure of sets of lattice points in the plane, having a small doubling property. Let $\mathbb{K}$ be a finite subset of $\mathbb{Z}^2$ such that

$$|\mathbb{K} + \mathbb{K}| < 3.5|\mathbb{K}| - 7.$$

If $\mathbb{K}$ lies on three parallel lines, then the convex hull of $\mathbb{K}$ is contained in three compatible arithmetic progressions with the same common difference, having together no more than

$$|\mathbb{K}| + \frac{3}{4}\Big(|\mathbb{K}+\mathbb{K}| - \frac{10}{3}|\mathbb{K}| + 5\Big)$$

terms. This upper bound is best possible.

In this note we classify the non-solvable finite groups G such that the class number of G is at least $|G|/16$. Some consequences are derived as well.

Some questions on small subsets in groups are posed and discussed.

The paper is devoted to an investigation of two-generated groups such that the $m-$th power of the generating pair contains less than 2^m elements . It is proved, in particular, that if the cube of the generating pair contains less than 7 elements or its fourth power contains less than 11 elements, then the group is solvable. Otherwise, it is not necessarily solvable. The proofs use computer calculations.

We generalise some known addition theorems to non abelian groups and to the most general case of relations having a transitive group of automorphisms.

The classical proofs of addition theorems use local transformations due to Davenport, Dyson and Kempermann. We present a completely different method based on the study of some blocks of imprimitivity with respect to the automorphism group of a relation.

Several addition theorems including the finite $\alpha+\beta$-Theorem of Mann and a formula proved by Davenport and Lewis will be generalised to relations having a transitive group of automorphisms.

We study the critical pair theory in the case of finite groups. We generalise Vosper Theorem to finite not necessarily abelian groups.

Chowla, Mann and Straus obtained in 1959 a lower bound for the size of the image of a diagonal form on a prime field. This result was generalised by Tietäväienen to finite fields with odd characteristics. We use our results on the critical pair theory to generalise this lower bound to an arbitrary division ring.

Our results apply to the superconnectivity problems in networks. In particular we show that a loopless Cayley graph with optimal connectivity has only trivial minimum cuts when the degree and the order are coprime.

New results on subset multiplication in groups
MARCEL HERZOG 309

This paper presents results and open problems related to the following topics: group with deficient multiplication sub-tables, product bases in finite groups.

On small sumsets in abelian groups
VSEVOLOD F. LEV 317

In this paper we investigate the structure of those pairs of finite subsets of an abelian group whose sums have relatively few elements: $|A+B| < |A|+|B|$. In 1960, J. H. B. Kemperman gave an exhaustive but rather sophisticated description of recursive nature. Using intermediate results of Kemperman, we obtain below a description of another type. Though not (generally speaking) sufficient, our description is intuitive and transparent and can be easily used in applications.

An analog of Freiman's theorem in groups
IMRE Z. RUZSA 323

It is proved that in a commutative group G, where the order of elements is bounded by an integer r, any set A having n elements and at most αn sums is contained in a subgroup of size Cn with $C = f(r, \alpha)$ depending on r and α but not on n. This is an analog of a theorem of G. Freiman which describes the structure of such sets in the group of integers.

Subset sums and coding theory
GÉRARD COHEN & GILLES ZÉMOR 327

We study some additive problems in the group $(\mathbb{Z}/2\mathbb{Z})^r$. Our purpose is to show how those problems are closely related to coding theory. We present some relevant classical coding techniques and make use of them to obtain some original contributions.

New Structural Approach to Integer Programming: a Survey
MARK CHAIMOVICH 341

The survey discusses a new approach to Integer Programming which is based on the structural characterization of problems using methods of additive number theory. This structural characterization allows one to design algorithms which are applicable in a narrower, yet still wide, domain of problems, and substantially improve the time boundary of existing algorithms. The new algorithms are polynomial for the class of problems in which they are applicable, and even linear ($O(m)$) for a wide class of the Subset-Sum and

Value-Independent Knapsack problems. Previously known polynomial time algorithms for the same classes of problems are at least two orders of magnitude slower.

New Algorithm for Dense Subset-Sum Problem
MARK CHAIMOVICH 363

A new algorithm for the dense subset-sum problem is derived by using the structural characterization of the set of subset-sums obtained by analytical methods of additive number theory. The algorithm works for a large number of summands (m) with values that are bounded from above. The boundary (ℓ) moderately depends on m. The new algorithm has $O(m^{7/4}/\log^{3/4} m)$ time boundary that is faster than the previously known algorithms the best of which yields $O(m^2/\log^2 m)$.

On the Two-Dimensional Subset Sum Problem
ALAIN PLAGNE 375

We consider a system of two linear boolean equations. Using methods from analytic number theory, we obtain sufficient conditions ensuring the solvability of the system. This completes Freiman's work on the subject.

On series of discrete random variables, 1: real trinomial distributions with fixed probabilities
JEAN-MARC DESHOUILLERS, GREGORY A. FREIMAN & WILLIAM MORAN .. 411

This paper begins the study of the local limit behaviour of triangular arrays of independent random variables $(\zeta_{n,k})_{1\leq k\leq n}$ where the law of $\zeta_{n,k}$ depends on on n. We consider the case when $\zeta_{n,1}$ takes three integral values $0 < a_1(n) < a_2(n)$ with respective probabilities p_0, p_1, p_2 which do not depend on n. We show three types of limit behaviours for the sequence of r. v. $\eta_n = \zeta_{n,1} + \cdots + \zeta_{n,n}$, according as $a_2(n)/\gcd(a_1(n), a_2(n))$ tends to infinity slower, quicker or at the same speed as $\sqrt{n}$.

On Bounds for the Concentration Function. 1
JEAN-MARC DESHOUILLERS, GREGORY A. FREIMAN & ALEXANDER A. YUDIN
..... 425

We give an upper bound for the concentration function of a sum of independent identically distributed integral valued random variables in terms of a lower bound for their tail, under the necessary extra condition that the random variables are not essentially supported in a proper arithmetic progression.