ISSN 2220-5438

Reprint from

Moscow Journal of Combinatorics and Number Theory

URSS

МФТИ

Volume 7 • Issue 1 2017

Moscow Journal of Combinatorics and Number Theory Volume 7 • Issue 1 2017

URSS

Moscow Journal
of Combinatorics
and Number Theory
2017, vol. 7, iss. 1,
pp. 73–78, [pp. 73–78]

Restricted Product Sets under Unique Representability

Fedor Petrov (St. Petersburg)

Abstract: Let A and B be non-empty subsets of a multiplicative abelian group. The well-known Kemperman–Scherk theorem says that if there is an element c with a unique representation as $c = ab$ $(a \in A, b \in B)$, then $|A \cdot B| \geqslant |A| + |B| - 1$. We obtain lower bounds on the restricted product sets $A \dot{\times} B = \{a \cdot b : a \in A, b \in B, a \neq b\}$ under similar assumptions. Our method works for the groups that can be embedded, additively or multiplicatively, into a field; in particular, for cyclic groups. The proofs use the polynomial method.

Keywords: restricted sumset, Kemperman—Scherk theorem, polynomial method

AMS Subject Classification: 05B10, 11B13

Received: 01.01.2016; **revised:** 27.06.16

Recall a classical theorem by Scherk [15] and Kemperman [8, 9] (see the history of this result in [12]):

THEOREM 1. *Let A, B be two finite subsets of some abelian group G. Assume that some element $c \in A \cdot B$ has unique representation as $c = ab$, $a \in A, b \in B$. Then $|A \cdot B| \geqslant |A| + |B| - 1$.*

This result was proved by purely combinatorial methods, that is, by Dyson changes: (A, B) is replaced by (A, xB) for appropriate $x \in G$, which is in turn replaced by $(A \cap xB, A \cup xB)$.

Consider now the simplest restricted version. Denote

$$A\dot{\times}B = \{ab : a \in A, b \in B, a \neq b\}.$$

For the additive group G we use the sign $\dot{+}$.

We use the polynomial method, in particular, the following useful corollary [2] of Alon's Combinatorial Nullstellensatz [1]:

THEOREM 2 (ALON—FÜREDI). *If X, Y are finite non-empty subsets of a field K, and the values of a polynomial $f \in K[x, y]$ are equal to 0 at all points of the grid $X \times Y$ but one, then* $\deg f \geqslant |X| + |Y| - 2$. *In particular, if k lines cover all but one points of $X \times Y$, then $k \geqslant |X| + |Y| - 2$.*

Theorem 2 have been recently generalized to polynomials over rings [3, 4], but we do not see how to apply it to the restricted addition or multiplication in rings. Condition (D) of the cited papers looks too strong at least for immediate applications.

We deduce Theorem 2 from the following formula which expresses the coefficient of $x^{|A|-1}y^{|B|-1}$ for any polynomial $f(x, y)$, $\deg f(x, y) \leqslant |A| + |B| - 2$:

$$[x^{|A|-1}y^{|B|-1}]f(x, y) = \sum_{t\in A, s\in B} \frac{f(t, s)}{\prod_{\tau\in A\setminus t}(t - \tau)\prod_{\xi\in B\setminus s}(s - \xi)}. \tag{1}$$

Indeed, if $\deg f < |X| + |Y| - 2$ in Theorem 2, then one can apply (1) for the polynomial $f(x, y)$ and the sets $X = A$, $Y = B$: LHS of (1) equals to 0, while in RHS there exists the unique non-zero summand.

The formula (1) can be naturally extended for d-dimensional grids $A_1 \times \ldots \times A_d$.

We should say few words about the history of this formula. Recently this formula was rediscovered in several combinatorial papers [6, 11, 14]. First of these papers is written by Uwe Schauz, it contains many interesting generalizations and corollaries.

But from algebraic geometry point of view (1) is just a specialization of the so called *Euler–Jacobi formula* for complete intersections [5] (the grid $A \times B$ is a complete intersection of the varieties $\prod_{a\in A}(x - a) = 0$, $\prod_{b\in B}(y - b) = 0$). For example see modern exposition and generalizations in [10]. We have not seen this specialization stated explicitly in algebraic papers, but we are not aware of them so much to make any strong statements.

Further we need the formula (1) itself. The following result is close to the result from [13] (the difference is that here we consider the number of representations $c = a + b$, $a \neq b$, while Pan and Sun count all representations $c = a + b$).

THEOREM 3. *Let A, B be two finite subsets of the additive group of a field. Assume that some element $c \in A \dot{+} B$ has the unique representation as $c = a + b$, $a \in A, b \in B$, $a \neq b$. Then $|A \dot{+} B| \geqslant |A| + |B| - 2$.*

PROOF. Assume the contrary. Consider $|A \dot{+} B|$ lines $x = y$ and $x + y = \gamma$, $\gamma \in (A \dot{+} B) \setminus c$. They cover all points of $A \times B$ except (a, b). Hence $|A \dot{+} B| \geqslant |A| + |B| - 2$ by Theorem 2. □

As it was noted by one of the referees, Theorem 3 is not a direct corollary of the results from [13], that is, it gives better estimates for some pairs of sets. But the proof does not differ.

COROLLARY 4. *Let A be a finite subset of the additive group of a field. Assume that some element $c \in A \dot{+} A$ has exactly two (symmetric to each other) representations as $c = a + b = b + a$, $a, b \in A$, $a \neq b$. Then $|A \dot{+} A| \geqslant 2|A| - 3$.*

PROOF. Denote $B = A \setminus a$ and apply Theorem 3. □

This result is sharp for $A = \{0, 1, 2, \ldots, |A| - 1\}$, $a = 0, b = 1$, when the characteristic of the field is equal to 0 or exceeds $2|A| - 3$. Analogous examples for Theorem 3 are given by the sets $A = \{0, 1, \ldots, |A| - 1\}$, $B = \{1, 2, \ldots, |B|\}$. We do not know whether essentially different examples of sharpness exist.

Now consider the case of the multiplicative group of a field. This consideration may be a useful approach for studying cyclic groups (recall that finitely generated abelian groups which may be embedded into multiplicative group of a field are those with cyclic torsion.) In the context of restricted sumsets/product sets his approach comes from [7].

The estimate becomes slightly worse:

THEOREM 5. *Let A, B be two finite subsets of the multiplicative group of a field. Assume that some element $c \in A \dot{\times} B$ has the unique representation as $c = ab$, $a \in A, b \in B$, $a \neq b$. Then $|A \dot{\times} B| \geqslant |A| + |B| - 3$.*

PROOF. The polynomial $(xy-1)\prod_{\gamma\in(A\dot\times B)\setminus c}(x-\gamma y)$ vanishes at all points of $(A\times B^{-1})\setminus(a,b^{-1})$, but not at (a,b^{-1}). Hence by Theorem 2 its degree $|A\dot\times B|+1$ is not less than $|A|+|B|-2$. □

Note that this bound cannot be improved, in general. For example, take the sets $A=\{1,w,\dots,w^{n-1}\}$, $B=\{1,w,\dots,w^{n-2}\}$, where $w^{2n-4}=1$, and w is a primitive root of 1 of order $2n-4$. Then $|A|=n$, $|B|=n-1$, $|A\dot\times B|=2n-4$ and 1 has the unique representation $w^{n-1}\cdot w^{n-3}$.

COROLLARY 6. *Let A be a finite subset of the multiplicative group of a field. Assume that some element $c\in A\dot\times A$ has exactly two (symmetric to each other) representations as $c=ab=ba$, $a,b\in A$, $a\neq b$. Then $|A\dot\times A|\geqslant 2|A|-4$.*

PROOF. Take $B=A\setminus b$ and apply Theorem 5. □

This result partially supports a conjecture due to V. Lev [12].

The example of $A=\{1,w,\dots,w^{n-1}\}$, $w^{2n-4}=1$, proves that this bound is sharp.

However, this result may be improved in the particular case, when $a^{n-2}\neq b^{n-2}$, where $n=|A|$ (this is not the case for our previous example):

THEOREM 7. *Let A be a finite subset of the multiplicative group of a field, $|A|=n$. Assume that some element $c\in A\dot\times A$ has exactly two (symmetric to each other) representations as $c=ab=ba$, $a,b\in A$, $a\neq b$. Assume also that $a^{n-2}\neq b^{n-2}$. Then $|A\dot\times A|\geqslant 2n-3$.*

PROOF. Assume that $|A\dot\times A|\leqslant 2n-4$, then $n\geqslant 3$ and $1\leqslant|(A\dot\times A)\setminus c|\leqslant 2n-5$. Let $\gamma_1,\dots,\gamma_{2n-5}$ be (not necessary distinct) elements such that $\{\gamma_1,\dots,\gamma_{2n-5}\}=$ $=(A\dot\times A)\setminus c$.

The polynomial

$$f(x,y):=(xy-1)\prod_{i=1}^{2n-5}(x-\gamma_i y)$$

of degree $2n-3$ vanishes at all points of $A\times A^{-1}$ except (a,b^{-1}) and (b,a^{-1}). We calculate the coefficient of $x^{n-1}y^{n-1}$-term by formula (1):

$$[x^{n-1}y^{n-1}]f(x,y)=\sum_{t\in A,s\in A^{-1}}\frac{f(t,s)}{\prod_{\tau\in A\setminus t}(t-\tau)\prod_{\xi\in A^{-1}\setminus s}(s-\xi)}.$$

We have two non-zero summands corresponding to points $(t, s) = (a, b^{-1})$ and $(t, s) = (b, a^{-1})$. The first of them is equal to

$$\frac{(ab^{-1}-1)\prod_i(a-\gamma_i b^{-1})}{\prod_{\tau\in A\setminus a}(a-\tau)\prod_{\xi\in A^{-1}\setminus b^{-1}}(b^{-1}-\xi)} =$$
$$(a-b)b^{4-2n}\frac{\prod_i(ab-\gamma_i)}{(-1)^{n-1}\prod_{\tau\in A\setminus a}(a-\tau)\prod_{\xi\in A^{-1}\setminus b^{-1}}b^{-1}\xi(b-\xi^{-1})} =$$
$$(a-b)b^{2-n}(-1)^{n-1}\frac{\prod_i(ab-\gamma_i)}{\prod_{\tau\in A\setminus a}(a-\tau)\prod_{\mu\in A\setminus b}(b-\mu)\prod_{\xi\in A^{-1}}\xi}.$$

The second summand has an analogous expression, one should just change a and b. We see that their sum is not equal to 0 provided that $a^{n-2} \neq b^{n-2}$. This is a contradiction. □

This bound is also sharp, for example, for $A = \{1, w, \dots, w^{n-1}\}$, $a = w^{n-1}$, $b = w^{n-2}$, if $w^k \neq 1$ for all $k = 1, 2, \dots, 2n-4$.

Lev posed an interesting question to estimate $|A\dot{\times}B|$, provided that $A\dot{\times}B \neq A \times B$. What we managed to prove here in this direction (for the multiplicative group of a field) is in most cases weaker than his conjecture:

THEOREM 8. *Let* $N = |\{a \in A \cap B : a^2 \notin A\dot{\times}B\}|$. *Then* $|A\dot{\times}B| \geqslant |A| + |B| - 2 - [N/2]$.

PROOF. For any $\gamma \in A\dot{\times}B$ consider the line $x = \gamma y$. All these lines cover all points of $A \times B^{-1}$ except N points (a, a^{-1}) on the hyperbola $xy = 1$. One should add $[N/2]$ lines covering all those points except one (this is clearly possible) and apply Theorem 2. □

Acknowledgements

I am deeply grateful to Gyula Károlyi and Vsevolod Lev for fruitful discussions, and to the anonymous referees, who suggested numerous improvements of the text.

Bibliography

1. ***N. Alon,*** *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), 7–29.
2. ***N. Alon, Z. Füredi,*** *Covering the cube by affine hyperplanes*, Eur. J. Comb. **14** (1993), 79–83.

3. ***A. Bishnoi, P. L. Clark, A. Potukuchi, J. R. Schmitt,*** *On Zeros of a Polynomial in a Finite Grid*, arXiv:1508.06020.
4. ***P. L. Clark,*** *Fattening Up Warning's Second Theorem*, arXiv:1506.06743.
5. ***K. G. Jacobi,*** *Theoremata nova algebraica circa systema duarum aequationum inter duas variabiles propositarum*, J. Reine Angew. Math. **14** (1835), 281–288.
6. ***R. N. Karasev, F. V. Petrov,*** *Partitions of nonzero elements of a finite field into pairs*, Israel J. Math. **192**:1 (2012), 143–156.
7. ***G. Károlyi,*** *The Erdős–Heilbronn problem in abelian groups*, Israel J. Math. **139**:1 (2004), 349–359.
8. ***J. H. B. Kemperman,*** *On complexes in a semigroup*, Indag. Math. **18** (1956), 247–254.
9. ***J. H. B. Kemperman,*** *On small sumsets in an abelian group*, Acta Math. **103** (1960), 63–88.
10. ***E. Kunz, M. Kreuzer,*** *Traces in strict Frobenius algebras and strict complete intersections*, J. Reine Angew. Math. **381** (1987), pp. 181–204.
11. ***M. Lasoń,*** *A generalization of Combinatorial Nullstellensatz*, Electron. J. Combin. **17**:1 (2010) #N32, 6 p.
12. ***V. Lev,*** *Restricted set addition in abelian groups*: *results and conjectures*, J. Th. Nombres. Bordeaux **17**:1 (2005), 181–193.
13. ***H. Pan, Z.-W. Sun,*** *Restricted sumsets and a conjecture of Lev*, Israel J. Math. **154**:1 (2006), 21–28
14. ***U. Schauz,*** *Algebraically solvable problems*: *describing polynomials as equivalent to explicit solutions*, Electron. J. Combin. **15** (2008) #R10, 35 p.
15. ***P. Scherk,*** *Distinct elements in a set of sums* (*solution to Problem* 4466), American Math. Monthly **62**:1 (1955), 46–47.

Fedor Petrov

St. Petersburg Department of
V. A. Steklov Institute of Mathematics of
the Russian Academy of Sciences,
St. Petersburg State University,
St. Petersburg, Russia
fedyapetrov@gmail.com