# On the length of arithmetic progressions in linear combinations of $S$-units

Lajos Hajdu and Florian Luca

*To Professors A. Pethő and J. Pintz on the occasion of their 60th birthdays*

**Abstract.** Recent finiteness results concerning the lengths of arithmetic progressions in linear combinations of elements from finitely generated multiplicative groups have found applications to a variety of problems in number theory. In the present paper, we significantly refine the existing arguments and give an explicit upper bound on the length of such progressions.

**Mathematics Subject Classification (2000).** Primary 11B25; Secondary 11D61.

**Keywords.** Arithmetic progressions, finitely generated groups, $S$-unit equations, subspace theorem.

## 1. Introduction and the main result

Linear equations involving elements from a finitely generated multiplicative group $\Gamma$, such as $S$-unit equations for example, are very important in many Diophantine problems. For the theory and applications of such and related equations we refer to [3, 4, 5, 6, 7, 8], and the references therein. Recently, Hajdu [9], and Jarden and Narkiewicz [10], independently, have investigated arithmetic progressions in the linear combinations of elements from such groups $\Gamma$. Their results had found several applications to Diophantine problems. To present these results and their applications as well as to clarify our aims, we first need to introduce some notation.

Let $K$ be an algebraically closed field of characteristic zero. Write $K^*$ for the multiplicative group of the nonzero elements of $K$, and let $\Gamma$ be a multiplicative subgroup of $K^*$ of finite rank $r$. Avoiding the trivial case, throughout the paper

L. H. was supported in part by the Hungarian Academy of Sciences and by the OTKA grants K67580 and K75566. F. L. was supported in part by Grants SEP-CONACyT 79685 and PA-PIIT 100508. Both authors were also supported in part by CONACyT and NKTH in the frame of the joint Mexican-Hungarian project "Diophantine equations and their applications in Cryptography".

we shall assume that $r > 0$. Note that for $r = 0$ our result is obviously true. Let $t$ be a positive integer, and let $\mathcal{A}$ be a finite, nonempty subset of $K^t$ having $n$ elements. Put

$$H_t(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^{t} a_i x_i : (a_1, \dots, a_t) \in \mathcal{A},\ (x_1, \dots, x_t) \in \Gamma^t \right\}.$$

Let $L$ be the length of the longest nonconstant arithmetic progression in $H_t(\Gamma, \mathcal{A})$. Hajdu [9], showed that this number is finite, and that it can be bounded in terms of $r,\ t$ and $n$. A similar result with somewhat more special settings (e.g., assuming $n = 1$ and $\mathcal{A} = \{(1, \dots, 1)\}$) has been obtained by Jarden and Narkiewicz [10]. Although recent, these results have already found many applications to problems coming from different parts of number theory: to the so-called unit sum number problem (see [10]), to a question of M. Pohst about representing primes as sums or differences of powers of 2 and 3 (see [9]), and to bound the lengths of arithmetic progressions in the solution sets of norm form equations (c.f. [2]).

Interestingly, aside from a result of Evertse, Schlickewei and Schmidt [6] on the number of nondegenerate solutions to linear equations with unknowns from a finitely generated group, the proofs of the theorems of Hajdu [9] and Jarden and Narkiewicz [10] are also based upon a classical result of van der Waerden [12] concerning monochromatic arithmetic progressions. Another common feature of the results of [9] and [10] is that the upper bounds for $L$ are not explicitly given. One could go through the above papers and write down an upper bound for $L$ based on their arguments, but since the proofs use van der Waerden's result, it is quite likely that the upper bound one would end up in this way with will be huge.

Our main result is an explicit upper bound for $L$ depending only on $r,\ t$ and $n$. Our argument is different from the ones from [9] and [10] and avoids the use of van der Waerden's theorem, and so it is clearly much smaller than the ones which would follow from the works [9] and [10]. We note that a relatively small, and completely explicit upper bound for $L$ is important also for the applications. For example, it becomes possible to make explicit the bound for the lengths of arithmetic progressions in the solution sets of norm form equations, given in [2].

**Theorem 1.1.** *With the above notation, we have*

$$L < \exp\left( (8(n+t+r))^{8(n+t+r)^4} \right). \tag{1.1}$$

## 2. Proof of Theorem 1.1

To prove Theorem 1.1, we need two lemmas. The first one is due to Amoroso and Viada [1] and concerns the number of nondegenerate solutions to linear equations with variables from $\Gamma$. This result is a recent improvement of a result from [6]. Consider the equation

$$a_1 x_1 + \cdots + a_k x_k = 1, \tag{2.1}$$

where $a_1,\dots,a_k\in K^*$ and $x_1,\dots,x_k$ are unknowns from $\Gamma$. A solution $(x_1,\dots,x_k)$ to equation (2.1) is called *nondegenerate* if $\sum_{i\in J}a_ix_i\neq 0$ for all nonempty subsets $J$ of $\{1,\dots,k\}$.

**Lemma 2.1.** *Equation* (2.1) *has at most* $C(k,r):=(8k)^{4k^4(k+r+1)}$ *nondegenerate solutions* $(x_1,\dots,x_k)\in\Gamma^k$.

*Proof.* This is an immediate consequence of Theorem 6.2 in [1]. □

For the next lemma, which is an analogue of the well-known exchange theorem of Steinitz from linear algebra, we need the following notion. Let $H_1$ and $H_2$ be two subsets of $K^*$. We say that $H_1$ and $H_2$ are *multiplicatively independent* if for any $h_1\in H_1$, $h_2\in H_2$, and $z_1,z_2\in\mathbb{Z}$ we have $h_1^{z_1}h_2^{z_2}=1$ only for $z_1=z_2=0$.

**Lemma 2.2.** *Let* $\Gamma$ *be as above, and suppose that* $\alpha_1,\dots,\alpha_m$ *are multiplicatively independent elements of* $K^*$*, namely that*

$$\alpha_1^{z_1}\cdots\alpha_m^{z_m}=1\quad (z_j\in\mathbb{Z},\ j=1,\dots,m)$$

*only when* $z_1=\cdots=z_m=0$. *Then there exist indices* $j_1,\dots,j_{m-r}$ *such that* $\Gamma$ *and* $B$ *are multiplicatively independent, where*

$$B=\{\alpha_{j_1}^{z_1}\dots\alpha_{j_{m-r}}^{z_{j_{m-r}}}:z_1,\dots,z_{m-r}\in\mathbb{Z}\}.$$

*Proof.* Assume that $m>r$, otherwise we have nothing to prove. Since the rank of $\Gamma$ is $r$, there exists an index $j$ such that $\alpha_j\in K^*\setminus\Gamma$. Without loss of generality, we may assume that $j=1$, i.e. $\alpha_1\in K^*\setminus\Gamma$. Then we obviously have that $\Gamma$ and $B_1$ are multiplicatively independent, where $B_1=\{\alpha_1^{z_1}:z_1\in\mathbb{Z}\}$. Assume now that we have already chosen $j<m-r$ elements, say $\alpha_1,\dots,\alpha_j$, such that $\Gamma$ and $B_j$ are multiplicatively independent, where

$$B_j=\{\alpha_1^{z_1}\dots\alpha_j^{z_j}:z_1,\dots z_j\in\mathbb{Z}\}.$$

Obviously, $\Gamma B_j$ has rank $r+j$. Hence, there must exist an index $j'$ with $j<j'\le m$ such that $\Gamma B_j$ and $B_{j'}$ are multiplicatively independent, where $B_{j'}=\{\alpha_{j'}^{z_{j'}}:z_{j'}\in\mathbb{Z}\}$, because otherwise $\Gamma B_j$ would contain $m>r+j$ multiplicatively independent elements, which is impossible. The statement now follows by induction on $m$. □

Now we can prove our main result.

*Proof of Theorem* 1.1. As it is well-known, $K$ has a subring $R$ isomorphic to $\mathbb{Z}$. For simplicity, we will just assume that $R=\mathbb{Z}$. Let $s$ be a positive integer to be chosen later and let $H=\{p_1,\dots,p_{r+s}\}$ be the set of the first $r+s$ primes. Then, by Lemma 2.2, we have that there is a subset $Q=\{q_1,\dots,q_s\}$ of $H$ such that

$$H':=\{q_1^{\beta_1}\cdots q_s^{\beta_s}:\beta_1,\dots,\beta_s\in\mathbb{Z}\}$$

and $\Gamma$ are multiplicatively independent. Write

$$\mathcal{I}:=H'\cap\{1,\dots,L-1\}.$$

Assume that $y_0, y_1, \ldots, y_{L-1}$ is some nonconstant arithmetic progression in $H_t(\Gamma, \mathcal{A})$, where $L$ does not satisfy the desired inequality (1.1). Observe that for every $i \in \mathcal{I}$ we have

$$y_0 + i(y_1 - y_0) = y_i.$$

We may assume that $y_0 y_1$ is nonzero, otherwise we apply our argument for the progression $y'_0, \ldots, y'_{L-1}$ with $y'_j = y_{L-1-j}$ $(j = 0, \ldots, L-1)$ (observe that $L > 3$ since $L$ fails to satisfy inequality (1.1)). Thus, the above equation can be rewritten as

$$i(y_0 - y_1)/y_0 + y_i/y_0 = 1.$$

Hence, writing

$$y_i = \sum_{\ell=1}^{t} a_{\ell,i} x_{\ell,i},$$

where $(a_{1,i}, \ldots, a_{t,i}) \in \mathcal{A}$ and $x_{\ell,i} \in \Gamma$ for all $\ell = 1, \ldots, t$, we get

$$a'_{0,i} i + \sum_{\ell=1}^{t} a'_{\ell,i} x_{\ell,i} = 1, \tag{2.2}$$

where

$$a'_{0,i} = (y_0 - y_1)/y_0, \qquad a'_{\ell,i} = a_{\ell,i}/y_0.$$

Note that $a'_{0,i} \neq 0$ because $y_0 \neq y_1$. Equation (2.2) can be thought of as an equation of the shape (2.1) with unknowns in $\Gamma' = \Gamma H'$. (Observe that $i$ varies only inside $H$). For any solution, equation (2.2) splits into a disjoint union of nondegenerate equations (i.e., subequations having no proper zero subsums). Assume first that the nondegenerate subequation containing the 1 in the right hand side contains the variable $i$ corresponding to the index 0 in the left hand side. Then, by Lemma 2.1, for any $(a_{1,i}, \ldots, a_{t,i}) \in \mathcal{A}$ the number of choices for $i$ is

$$\leq C(t+1, r+s) = (8(t+1))^{4(t+1)^4(t+r+s+2)},$$

and the number of possibilities (i.e., subsets of indices involved) for the actual subequation is $< 2^t$. Assume now that the index 0 is not in the left hand side of the nondegenerate subequation containing 1 on the right hand side. This means that the nondegenerate equation that $i$ is involved in looks like

$$a'_{0,i} i + \sum_{\ell \in \mathcal{L}} a'_{\ell,i} x_{\ell,i} = 0, \tag{2.3}$$

for some nonempty subset $\mathcal{L}$ of $\{1, \ldots, t\}$. This can be rewritten as

$$\sum_{\ell \in \mathcal{L}} \hat{a}_{\ell,i} \hat{x}_{\ell,i} = 1,$$

where $\hat{a}_{\ell,i} := -a'_{\ell,i}/a'_{0,i}$, $\hat{x}_{\ell,i} := x_{\ell,i}/i$. By Lemma 2.1, there are only at most

$$C(t, r+s) = (8t)^{4t^4(t+r+s+1)}$$

such solutions for any $(a_{1,i},\dots,a_{t,i})\in\mathcal{A}$. Given any of the numbers $\hat{x}_{\ell,i}$ for a solution, $i$ is uniquely recovered since $i\in\mathcal{I}\subset H'$, and $\Gamma$ and $H'$ are multiplicatively independent. Again, the number of possibilities for the set $\mathcal{L}$ is $<2^t$.

Putting everything together, we see that all $i\in\mathcal{I}$ occurs as a solution of either (2.2) or of (2.3). Since $|\mathcal{A}|=n$, the vector $(a_{1,i},\dots,a_{t,i})$ can be chosen in at most $n^t$ ways. Thus, the number of possible equations both of the form (2.2) and of the shape (2.3) is $<(2n)^t$. Hence, it follows that

$$|\mathcal{I}|<n^t2^{t+1}(8(t+1))^{4(t+1)^4(t+r+s+2)}. \tag{2.4}$$

A good lower bound for $|\mathcal{I}|$ in terms of $L$ is the cardinality of the set of positive integers $i\le L-1$ which are divisible only by primes $p_{r+1},\dots,p_{r+s}$, where $p_\ell$ stands for the $\ell$th prime number. Let $\omega:=\lfloor\log(L-1)/\log p_{r+s}\rfloor$. Then

$$|\mathcal{I}|\ge\binom{\omega+s}{s}\ge\left(\frac{e\omega}{s}\right)^s, \tag{2.5}$$

provided that $\omega>s$, which we check below. In the last inequality above we used the fact that $s!\ge(s/e)^s$. Further, to see the first inequality in (2.5) above, observe that the binomial coefficient in (2.5) counts the number of $s$-tuples of nonnegative integers $(\beta_1,\dots,\beta_s)$ such that $\beta_1+\cdots+\beta_s\le\omega$. Indeed, putting $\gamma_i=\sum_{j=1}^i(\beta_j+1)$, then $1\le\gamma_1<\cdots<\gamma_s\le\omega+s$, and the above binomial coefficient is the exact count for the number of $s$-tuples of $\gamma_i$'s. Since $\beta_i=\gamma_i-\gamma_{i-1}-1$ (with $\gamma_0:=0$ by convention), we have a one-to-one correspondence between the $s$-tuples of $\beta_i$'s and the $s$-tuples of $\gamma_i$'s. Clearly, for each $s$-tuple of $\beta_i$'s, the number $q_1^{\beta_1}\cdots q_s^{\beta_s}$ is $\le L-1$ so it belongs to $\mathcal{I}$, and distinct $s$-tuples of $\beta_i$'s give rise to distinct members of $\mathcal{I}$ by unique factorization.

Let us now check that $\omega\ge s$. Assuming also that $s>\max\{2,r\}$, we have that

$$p_{r+s}<p_{2s}\le 4s\log(4s)<s^3.$$

For the above inequality, we used known effective estimates concerning the size of the $\ell$th prime (see [11], for example). In fact, the very last inequality above actually fails for $s=3$, but in this case we have that inequality $p_{r+s}\le p_5=11<27=3^3$ holds true nevertheless. Clearly, $L-1>L^{1/2}$ for $L>2$, therefore

$$\frac{\log(L-1)}{\log p_{r+s}}>\frac{\log L}{6\log s},$$

so that $\omega\ge(\log L)/(12\log s)$. Hence, the inequality $\omega\ge s$ is implied by $\log L>12s\log s$, which in turn is implied by $\log L>12s^2$. Hence, assuming that $s\ge3$ and that $\log L\ge12s^2$, everything works out and we get that

$$\frac{e\omega}{s}>\frac{\log L}{6s\log s}, \tag{2.6}$$

because $e>2$. Now estimate (2.5) implies that

$$|\mathcal{I}|>\left(\frac{\log L}{6s\log s}\right)^s.$$

Comparing the above lower bound with inequality (2.4), we arrive at

$$\log L < 6s(\log s)n^{t/s}2^{(t+1)/s}(8(t+1))^{4(t+1)^4(t+r+s+2)/s}.$$

Now take $s = n + t + r$. Using that $n, t, r$ are all positive whence $s \geq 3$, we get

$$\log L < 6s(\log s)(s-2)2^{1-1/s}(8(s-1))^{4(s-1)^4(2+1/s)} < (8s)^{4(s-1)^4(2+1/s)+3}.$$

A simple calculation shows that we have

$$4(s-1)^4(2+1/s)+3 < 8s^4.$$

This implies that

$$\log L < (8s)^{8s^4},$$

and the desired inequality follows. □

## References


[1] F. Amoroso and E. Viada, *Small points on subvarieties of a torus.* Duke Math. J. **150** (2009), 407–442.

[2] A. Bérczes, L. Hajdu and A. Pethő, *Arithmetic progressions in the solution sets of norm form equations.* Rocky Mountain J. Math. (to appear).

[3] J.-H. Evertse and K. Győry, *On unit equations and decomposable form equations.* J. Reine Angew. Math. **358** (1985), 6-19.

[4] J.-H. Evertse, K. Győry, C. Stewart and R. Tijdeman, *S-unit equations and their applications.* New Advances in Transcendence Theory (A. Baker, ed.), Cambridge University Press, Cambridge, 1988, pp. 110-174.

[5] J.-H. Evertse and H. P. Schlickewei, *The absolute subspace theorem and linear equations with unknowns from a multiplicative group.* Number theory in progress, Vol. 1 (Zakopane-Koscielisko, 1997), de Gruyter, Berlin, 1999, pp. 121-142.

[6] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group.* Annals Math. **155** (2002), 807–836.

[7] K. Győry, *Some recent applications of S-unit equations.* Astérisque **209** (1992), 17-38.

[8] K. Győry, *Solving Diophantine equations by Bakers theory.* A panorama of number theory or the view from Bakers garden (Zürich, 1999), Cambridge Univ. Press, Cambridge, 2002, pp. 38–72.

[9] L. Hajdu, *Arithmetic progressions in linear combinations of S-units.* Period. Math. Hung. **54** (2007), 51–61.

[10] M. Jarden and W. Narkiewicz, *On sums of units.* Monatsh. Mat. **150** (2007), 327–332.

[11] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers.* Illinois J. Math. **6** (1962), 64–94.

[12] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung.* Nieuw Archief voor Wiskunde **19** (1927), 212–216.

**Acknowledgment**

The authors are grateful to the referee for his/her helpful suggestions and remarks.

Lajos Hajdu
University of Debrecen
Institute of Mathematics
and the Number Theory Research Group
of the Hungarian Academy of Sciences
P.O. Box 12
H-4010 Debrecen
Hungary
e-mail: hajdul@math.klte.hu

Florian Luca
Mathematical Institute, UNAM
Ap. Postal 61–3 (Xangari), CP 58 089
Morelia, Michoacán
Mexico
e-mail: fluca@matmor.unam.mx