Journal of Number Theory 208 (2020) 168–179

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

On the minimal Hamming weight of a multi-base representation

Daniel Krenn [a,*,1], Vorapong Suppakitpaisarn [b], Stephan Wagner [c,2]

[a] *Department of Mathematics, Alpen-Adria-Universität Klagenfurt, Universitätsstraße 65–67, 9020 Klagenfurt, Austria*
[b] *Graduate School of Information Science and Technology, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*
[c] *Department of Mathematical Sciences, Stellenbosch University, Private Bag X1, Matieland 7602, South Africa*

ARTICLE INFO

Article history:
Received 20 August 2018
Received in revised form 12 July 2019
Accepted 12 July 2019
Available online 27 August 2019
Communicated by S.J. Miller

MSC:
11A63
11J25
68R05
94A15

Keywords:
Multi-base representations
Hamming weight
Minimal weight

ABSTRACT

Given a finite set of bases b_1, b_2, ..., b_r (integers greater than 1), a multi-base representation of an integer n is a sum with summands $db_1^{\alpha_1} b_2^{\alpha_2} \cdots b_r^{\alpha_r}$, where the α_j are nonnegative integers and the digits d are taken from a fixed finite set. We consider multi-base representations with at least two bases that are multiplicatively independent. Our main result states that the order of magnitude of the minimal Hamming weight of an integer n, i.e., the minimal number of nonzero summands in a representation of n, is $\log n/(\log\log n)$. This is independent of the number of bases, the bases themselves, and the digit set.

For the proof, the existing upper bound for prime bases is generalized to multiplicatively independent bases; for the required analysis of the natural greedy algorithm, an auxiliary result in Diophantine approximation is derived. The lower bound follows by a counting argument and alternatively by using communication complexity; thereby improving the existing bounds and closing the gap in the order of magnitude.

* Corresponding author.
E-mail addresses: math@danielkrenn.at, daniel.krenn@aau.at (D. Krenn), vorapong@is.s.u-tokyo.ac.jp (V. Suppakitpaisarn), swagner@sun.ac.za (S. Wagner).

[1] Daniel Krenn is supported by the Austrian Science Fund (FWF): P 28466-N35.
[2] Stephan Wagner is supported by the National Research Foundation of South Africa, grant 96236.

https://doi.org/10.1016/j.jnt.2019.07.023

This implies also that the greedy algorithm terminates after $\mathcal{O}(\log n/\log\log n)$ steps, and that this bound is sharp.

1. Introduction

1.1. Multi-base representations

Let a finite set $\{b_1, b_2, \ldots, b_r\}$ of *bases* (integers greater than 1) be given, along with a finite set D of nonnegative integers that includes 0. The elements of D will be called *digits*. We let

$$\mathcal{B} = \left\{ b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_r^{\alpha_r} \;\middle|\; \alpha_1,\ \alpha_2, \ldots, \alpha_r \text{ nonnegative integers} \right\}$$

be the free monoid generated by b_1, b_2, $\ldots$, b_r; the elements of $\mathcal{B}$ are called *power-products*. A *multi-base representation* of a positive integer n is a representation of the form

$$n = \sum_{B\in\mathcal{B}} d_B B, \tag{$\circledast$}$$

where $d_B \in D$ for all $B \in \mathcal{B}$.

For simplicity, we make the natural assumption that every positive integer has at least one such representation, which implies in particular that $1 \in D$. We will also assume that the bases b_1, b_2, $\ldots$, b_r are multiplicatively independent, i.e., the only integers α_1, α_2, $\ldots$, α_r for which

$$b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_r^{\alpha_r} = 1$$

are $\alpha_1 = \alpha_2 = \cdots = \alpha_r = 0$. Intuitively, this means that there is no "redundancy" in the set of bases.

Note that we obtain the standard base-b representation for $r = 1$, base $b_1 = b$ and digit set $D = \{0, 1, \ldots, b-1\}$.

1.2. Notes on the set-up

The set-up for multi-base representations that we described is quite standard (except possibly for the multiplicative independence). However, our proofs still apply with the following modifications:

- All digits d_B in the multi-base representations ($\circledast$) of n are assumed to be in $\mathcal{O}(\log n)$ (in contrast to a finite, nonnegative digit set).

- All exponents α_j in the multi-base representations ($\circledast$) of n are assumed to be in $\mathcal{O}(\log n)$. This is essentially trivial if all digits are nonnegative (see Section 1.7), but we can also allow negative digits if this additional assumption is imposed.
- At least two of the bases are assumed to be multiplicatively independent (in contrast to the entire set being multiplicatively independent).

1.3. Hamming weight

Of course, only finitely many terms of the sum ($\circledast$) can be nonzero. The number of these terms is called the *Hamming weight* of a representation. The Hamming weight is a measure of how efficient a certain representation is. A multi-base representation of an integer n is called *minimal* if it minimizes the Hamming weight among all multi-base representations of n with the same bases and digit set.

An overview on previous works concerning the Hamming weight of multi-base representations will follow in Sections 1.6 to 1.9. At this point, we only mention that the Hamming weight of single-base representations has been thoroughly studied (see Section 1.9), not only in the case of the standard set $\{0, 1, \ldots, b-1\}$ of digits, but also for more general types of digit sets. Both the worst case (maximum) and the average order of magnitude of the Hamming weight are $\log n$.

1.4. Main result

In this short note, we investigate the Hamming weight of multi-base representations and find that the Hamming weight can be reduced—even in the worst case—by using multi-base representations. However, the reduction compared to single-base representations is fairly small. Perhaps surprisingly, the order of magnitude is independent of the number r of bases (provided only that $r \geq 2$), the set of bases and the set of digits: it is always $\frac{\log n}{\log \log n}$.

The precise statement is as follows.

Theorem 1. *Suppose that $r \geq 2$, and that the multiplicatively independent bases b_1, b_2, $\ldots$, b_r and the digit set D are such that every positive integer n has a representation of the form ($\circledast$). There exist two positive constants K_1 and K_2 (depending on b_1, b_2, $\ldots$, b_r and D) such that the following hold:*

- (U) *For all integers $n > 2$, there exists a representation of the form ($\circledast$) with Hamming weight at most $K_1 \frac{\log n}{\log \log n}$.*
- (L) *For infinitely many positive integers n, there is no representation of the form ($\circledast$) whose Hamming weight is less than $K_2 \frac{\log n}{\log \log n}$.*

The upper bound of this theorem needs weaker assumptions on the bases than the result of Dimitrov, Jullien and Miller [12]: They require that all the bases b_1, $\ldots$, b_r are primes,[3] whereas we only need that (two of) the bases are multiplicatively independent. The order of magnitude of both bounds coincides. We will prove the bound (U) for our general multi-base set-up in Section 2 by analyzing the Greedy algorithm.

The best known lower bound[4] for the minimal Hamming weight seems to be of order $\frac{\log n}{\log\log n \cdot \log\log\log n}$ (see Dimitrov and Howe [10]) for double-base representations with bases 2 and 3. Yu, Wang, Li and Tian [30] extend this result to triple-base representations with bases 2, 3 and 5. Our lower bound (L) closes the gap to the upper bound in the order by getting rid of the factor $\log\log\log n$ in the denominator. We show this result in Section 3 by a counting argument and in Section 4 by using communication complexity.

1.5. Background on multi-base representations

Motivation for studying multi-base representations comes from fast and efficient arithmetical operations. One particular starting point is [12], where double-base and multi-base representations are used for modular exponentiation. Beside many other references, [2,11,13] describe the usage of double-base systems for cryptographic applications; the typical bases used are 2 and 3.

Questions such as: does every integer have a multi-base representation, or: what is the smallest number that cannot be represented in a certain system, are also of great interest; cf. [6,4,5,19]. The number of multi-base representations has also been analyzed; see [17,18].

1.6. Greedy algorithm

Let us come back to multi-base representations in this work's set-up. The natural greedy algorithm finds a multi-base representation of a nonnegative integer n successively by

- adding the largest power-product $B \in \mathcal{B}$ less than or equal to n to the representation, and
- continuing in the same manner with $n - B$.

The greedy algorithm does not produce a minimal representation in general. For instance, for double-base representations with bases 2 and 3, the smallest counter-example is

$$41 = 2^2 3^2 + 2^2 + 1 = 2^5 + 3^2.$$

[3] The proof of the bound in [12] is carried out for double-base representations with bases 2 and 3, and it is stated that it generalizes to sets of bases being finite sets of primes.

[4] When we speak of a "lower bound", say $L(n)$, in this paper, we mean that there exist infinitely many positive integers n which do not have a representation with Hamming weight less than $L(n)$.

The upper bound for the minimal Hamming weight is derived by Dimitrov, Jullien and Miller [12] by analyzing the greedy algorithm (as mentioned for prime bases). This is also our approach in this paper. Our result translates to the following corollary, which is a direct consequence of the proof and the statement of Theorem 1.

Corollary 2. *Suppose that $r \geq 2$, and that the multiplicatively independent bases b_1, b_2, ..., b_r and the digit set D are such that every positive integer n has a representation of the form (⁎). Then, the natural greedy algorithm with input n terminates after $\mathcal{O}\bigl(\frac{\log n}{\log\log n}\bigr)$ steps, and this bound is sharp. The output is a representation containing only digits 0 and 1.*

Note that this corollary is valid if the greedy algorithm is suitably preprocessed. To make this more precise, the algorithm needs representations with only digits 0 and 1 for all numbers from 0 to some N_0. This N_0 is to be found in the proof of Theorem 1, part (U); it might actually be huge (if it can even be calculated with reasonable effort). On the other hand, relaxing the condition on the digits being only 0 and 1 for the numbers up to N_0 also suffices for the validity of Corollary 2.

Yu, Wang, Li and Tian [30] use the proof of the $\mathcal{O}\bigl(\frac{\log n}{\log\log n}\bigr)$ bound of [12] for double-base representations with bases 2 and 3 to show the same bound for triple-base representations with bases 2, 3 and 5.

It is already mentioned in [12] that their upper bound of the Hamming weight of the representations obtained by the greedy algorithm is best possible. Such a lower bound is also derived in [8].

1.7. Lower bounds

Clearly, the minimal Hamming weight of integers $n \in \mathcal{B}$ is 1. So a goal related to lower bounds is to find sequences of integers with large minimal Hamming weight.

As mentioned, Dimitrov and Howe [10] and Yu, Wang, Li and Tian [30] state the existence of a constant K_2 and the existence of infinitely many integers n whose minimal Hamming weight is greater than $K_2 \frac{\log n}{\log\log n \cdot \log\log\log n}$ for representations with bases 2 and 3, and bases 2, 3 and 5, respectively.

1.8. Distribution of the Hamming weight

Beside the minimal Hamming weight of an integer n, the expected Hamming weight of a random multi-base representation of n and more generally the distribution of the Hamming weight of all representations of n have been studied. In [17,18], an asymptotic formula of the form $K(\log n)^r + \mathcal{O}\bigl((\log n)^{r-1}\log\log n\bigr)$ for the expected Hamming weight of a random representation of an integer n is derived with explicit constant K; see [18, Theorem IV]. The order of magnitude $(\log n)^r$ of this result depends, in contrast to the minimal Hamming weight, on the number r of bases. Moreover, it is shown in [17,18] that the Hamming weight asymptotically follows a Gaussian distribution, and an asymptotic expression for the variance is provided as well.

1.9. Single-base representations

For completeness, we also provide some background on (redundant) single-base representations, i.e., representations with $r = 1$ and an integer base $b_1 = b$, but a digit set that might differ from the standard choice $\{0, 1, \dots, b - 1\}$.

Papers [16] and [24] provide a way to compute minimal representations. The minimal Hamming weight of different kinds of single-base representations is studied in [9,22,23,26,27]. One particular representation, which often is minimal, is the so-called non-adjacent form (cf. [25,15]); it uses a signed digit set, i.e., a digit set containing also negative integers. Grabner and Heuberger [14] count representations with minimal Hamming weight for such a signed digit set.

2. The upper bound

The proof of the first statement of Theorem 1 follows from an analysis of the natural greedy algorithm and is based on some results from Diophantine approximation.

The following lemma is the statement corresponding to the result of Tijdeman [28] on which the analysis of Dimitrov, Jullien and Miller in [12] is based.

Lemma 3. *There are positive constants C and κ with the following property: for every integer $n > 1$, there is an element $B \in \mathcal{B}$ such that*

$$ne^{-C(\log n)^{-\kappa}} \leq B \leq n.$$

Proof. It clearly suffices to prove the statement in the case where $r = 2$; let us use the abbreviations $p = b_1$, $q = b_2$, and set $\lambda = \log_p q$. Since p and q are multiplicatively independent, λ is irrational, which will be crucial for us.

Let $\{x\} = x - \lfloor x \rfloor$ denote the fractional part of a real number x. As a first step, we consider the sequence $\Lambda_M = (\{\lambda m\})_{m=0}^{M-1}$ and show that its "gaps" (intervals that do not contain a value of Λ_M) can be bounded in terms of M. The structure of these gaps is in fact very well understood (see [1]), but we only require an upper bound.

Recall that the *discrepancy* of Λ_M is given by

$$D(\Lambda_M) = \sup_J \left| \frac{1}{M} |J \cap \Lambda_M| - \mu(J) \right|,$$

where μ denotes the Lebesgue measure and the supremum is taken over all intervals $J \subseteq [0, 1]$. The discrepancy is obviously an upper bound on the length of the largest gap in Λ_M (i.e., the Lebesgue measure of the largest interval J such that $|J \cap \Lambda_M| = 0$). Sequences of the form $(\{\lambda m\})_{m \geq 0}$ and their discrepancy have been investigated quite thoroughly: let γ be the *irrationality measure* of λ, which is defined as the infimum of all exponents ν for which there are at most finitely many integer solutions (a, b) to the inequality

$$\left|\lambda - \frac{a}{b}\right| < \frac{1}{b^\nu}.$$

Then one has $D(\Lambda_M) = \mathcal{O}\bigl(M^{-1/(\gamma-1)+\epsilon}\bigr)$ for every $\epsilon > 0$; see [20, Chapter 2.3, Theorem 3.2]. The fact that the irrationality measure γ is finite in our case, where $\lambda = \log_p q$, is a simple consequence of Baker's theory of linear forms in logarithms; see [3] for a general reference. Bugeaud [7] even provides explicit bounds for this specific case.

Fix a positive constant $\kappa < 1/(\gamma - 1)$ and a positive constant C_1 such that

$$D(\Lambda_M) \le C_1 M^{-\kappa}$$

for all $M \ge 1$. We set $M = \lceil \log_q n \rceil$ and consider the interval from $\{\log_p n\} - C_1 M^{-\kappa}$ to $\{\log_p n\}$. Since the discrepancy is an upper bound on all gaps in Λ_M, we know that there must be an $m \in \{0, 1, \dots, M - 1\}$ such that

$$\{\log_p n\} - C_1 M^{-\kappa} \le \{\lambda m\} \le \{\log_p n\}.$$

Note that if $\{\log_p n\} \le C_1 M^{-\kappa}$, we may simply choose $m = 0$.

Since $\lambda m \le \lambda(M - 1) \le \log_p q \log_q n = \log_p n$, it follows that there is a nonnegative integer ℓ such that

$$\log_p n - C_1 M^{-\kappa} \le \ell + \lambda m \le \log_p n,$$

which is equivalent to

$$\log n - (C_1 \log p) M^{-\kappa} \le \ell \log p + m \log q \le \log n.$$

This in turn implies that there exist nonnegative ℓ and m such that

$$n e^{-C(\log n)^{-\kappa}} \le p^\ell q^m \le n,$$

where $C = (C_1 \log p)(\log q)^\kappa$. This proves the lemma. $\square$

Now we are ready to prove statement (U) of Theorem 1.

Proof of Theorem 1, part (U). Take C and κ as in the lemma, and note that

$$\frac{\log(Cn/(\log n)^\kappa)}{\log\log(Cn/(\log n)^\kappa)} = \frac{\log n}{\log\log n} - \kappa + O\Bigl(\frac{1}{\log\log n}\Bigr).$$

Let N_0 be large enough so that $C/(\log n)^\kappa < \frac{1}{2}$ as well as

$$\frac{\log(Cn/(\log n)^{\kappa})}{\log\log(Cn/(\log n)^{\kappa})} \le \frac{\log n}{\log\log n} - \frac{\kappa}{2} \tag{1}$$

for all $n > N_0$. Moreover, choose a constant $K_1 \ge \frac{2}{\kappa}$ sufficiently large so that every positive integer $n \in \{3, 4, \dots, N_0\}$ has a representation of the form (⋇) of Hamming weight at most $\min\left\{\frac{K_1 \log n}{\log\log n}, \frac{K_1 \log N_0}{\log\log N_0}\right\}$.

Now it follows by induction that in fact every integer $n > 2$ has a representation whose Hamming weight is at most $\frac{K_1 \log n}{\log\log n}$. For $n \le N_0$, this holds by our choice of N_0 and K_1. For $n > N_0$, Lemma 3 guarantees the existence of an element $B \in \mathcal{B}$ for which

$$0 \le n - B \le n - ne^{-C(\log n)^{-\kappa}} \le \frac{Cn}{(\log n)^{\kappa}}. \tag{2}$$

The latter inequality follows by taking advantage of the classic bound $1 - e^{-x} \le x$. The number $n - B$ therefore has a representation whose Hamming weight is at most

$$K_1 \cdot \frac{\log(Cn/(\log n)^{\kappa})}{\log\log(Cn/(\log n)^{\kappa})} \le K_1 \frac{\log n}{\log\log n} - \frac{K_1\kappa}{2} \le K_1 \frac{\log n}{\log\log n} - 1$$

because of (1). The bound (2) and our assumption $C/(\log n)^{\kappa} < \frac{1}{2}$ imply $n - B \le Cn/(\log n)^{\kappa} < \frac{n}{2}$, so we must have $n - B < B$, thus the element B does not occur in the representation of $n - B$ (i.e., its coefficient d_B is zero). So we can add B to the representation of $n - B$ to obtain a multi-base representation of the form (⋇) whose Hamming weight is at most $\frac{K_1 \log n}{\log\log n}$. This completes the induction and thus the proof of the desired upper bound. □

3. The lower bound

The second statement (L) of Theorem 1 is proven by means of a simple counting argument. We will use the assumptions made in Section 1.2. Multiplicative independence is not actually required, though.

Note first that in any representation of the form

$$n = \sum_{B \in \mathcal{B}} d_B B,$$

with nonnegative $d_B \in D$, a digit d_B can only be nonzero if $B \le n$. The number B, on the other hand, can be represented as

$$B = b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_r^{\alpha_r}$$

for some nonnegative integers α_1, α_2, …, α_r by definition. We must have

$$0 \le \alpha_j \le \log_{b_j} B,$$

giving us $1 + \lfloor \log_{b_j} B \rfloor$ possible values for α_j. This justifies our assumption (Section 1.2) that the number of possible values of α_j is bounded by $c_j \log n$ for some constant c_j.

Proof of Theorem 1, part (L). For the moment, let N be an arbitrary positive integer; later, we will choose $N = 2^s$ and let $s \to \infty$. Let $\mathcal{B}_N \subseteq \mathcal{B}$ be the set of power-products appearing in some multi-base representation of some integer in the set $\{1, 2, \dots, N\}$. We head for a bound for $|\mathcal{B}_N|$. As mentioned, we have $d_B = 0$ for all $B > N$, so all such integers B do not contribute to multi-base representations of numbers in $\{1, 2, \dots, N\}$ and are therefore not contained in $\mathcal{B}_N$.

By the considerations above, we have

$$|\mathcal{B}_N| \le T(N) := \prod_{j=1}^{r} (c_j \log N) = (\log N)^r \prod_{j=1}^{r} c_j$$

as $N \to \infty$. The number $R_K(N)$ of representations using only the power-products in $\mathcal{B}_N$ and having Hamming weight at most K is bounded above by

$$R_K(N) \le \sum_{k=1}^{K} \binom{T(N)}{k} (|D| - 1)^k,$$

since we have at most $\binom{T(N)}{k}$ choices for those $B \in \mathcal{B}_N$ with nonzero digits d_B, and at most $(|D|-1)^k$ choices for the digits. A crude estimate gives us, at least for $K \le T(N)/2$,

$$\begin{aligned} R_K(N) &\le \binom{T(N)}{K} \sum_{k=1}^{K} (|D| - 1)^k \\ &\le \binom{T(N)}{K} |D|^K \\ &\le \bigl(|D|\, T(N)\bigr)^K. \end{aligned}$$

We claim that for every positive constant $K_2 < \frac{1}{r}$, the following holds: for all sufficiently large positive integers s, there is an integer $n \in \{2^{s-1} + 1, 2^{s-1} + 2, \dots, 2^s\}$ without a representation whose Hamming weight is less than $K_2 \frac{\log n}{\log \log n}$. This implies that there are infinitely many values of positive integers n for which there is no representation whose Hamming weight is less than or equal to $K_2 \frac{\log n}{\log \log n}$, completing the proof.

To prove the claim, suppose all integers in the set $\{2^{s-1} + 1, 2^{s-1} + 2, \dots, 2^s\}$ have a representation whose Hamming weight is at most K. Then we must have

$$\bigl(|D|\, T(2^s)\bigr)^K \ge R_K(2^s) \ge 2^{s-1}.$$

Taking logarithms yields

$$K \geq \frac{(s-1)\log 2}{\log T(2^s) + \log|D|} = \frac{(s-1)\log 2}{r\log s + \mathcal{O}(1)} > K_2 \frac{\log(2^s)}{\log\log(2^s)}$$

for sufficiently large s. The claim follows. □

4. From the point of view of communication complexity

In this section, we will provide an alternative proof based on communication complexity, to show that the upper bound obtained in Section 2 is asymptotically tight; i.e., we prove (L) of Theorem 1.

As mentioned, we use communication complexity to prove the statement. Consider the situation where Alice and Bob both hold ℓ bits of information (or equivalently a nonnegative integer less than 2^ℓ), denoted by the messages m_{Alice} and m_{Bob}. Bob wants to check if they hold the same information. To do that, Alice can send some message (according to some protocol) to Bob. Every time Bob got a bit of information from Alice, he can announce "equal" if he is sure that $m_{\text{Alice}} = m_{\text{Bob}}$, "not equal" when he is sure that $m_{\text{Alice}} \neq m_{\text{Bob}}$, or "more information" to request more information on m_{Alice} from Alice. Alice wants to minimize the number of bits that she sends to Bob; see Yao [29].

It is known that, when Alice uses any deterministic algorithm/protocol, there always exist messages m_{Alice} and m_{Bob} such that the number of communication bits is at least ℓ; see Kushilevitz [21].

For the proof below, we will use the assumptions made in Section 1.2, but again we do not require multiplicative independence.

Proof of Theorem 1, part (L). We assume for contradiction that for each n, there exists a multi-base representation with only $o\big(\frac{\log n}{\log\log n}\big)$ summands. Set $\ell = \lfloor \log n \rfloor$. Let m_{Alice} and m_{Bob} be ℓ-bit messages so that ℓ bits need to be communicated in order to determine equality.

Now, suppose that Alice converts the ℓ-bit message m_{Alice} to a multi-base representation with $o\big(\frac{\log n}{\log\log n}\big)$ summands. Since all exponents are in $\mathcal{O}(\log n)$ and the number r of bases is fixed, each summand of a multi-base representation can be denoted by $\mathcal{O}(\log\log n)$ bits. Therefore, Alice can tell Bob the whole message m_A by only

$$\mathcal{O}(\log\log n) \cdot o\Big(\frac{\log n}{\log\log n}\Big) = o(\log n)$$

bits; a contradiction. □

Acknowledgments

We thank Thatchaphol Saranurak (Toyota Technological Institute at Chicago) for suggesting us to use communication complexity in Section 4.

References

[1] Pascal Alessandri, Valérie Berthé, Three distance theorems and combinatorics on words, Enseign. Math. (2) 44 (1–2) (1998) 103–132.

[2] Roberto Avanzi, Vassil Dimitrov, Christophe Doche, Francesco Sica, Extending scalar multiplication using double bases, in: Advances in Cryptology—ASIACRYPT 2006, in: Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 130–144.

[3] A. Baker, Transcendental Number Theory, Cambridge University Press, Cambridge, 1990, etc.

[4] Csanád Bertók, Representing integers as sums or differences of general power products, Acta Math. Hungar. 141 (3) (2013) 291–300.

[5] Csanád Bertók, Lajos Hajdu, Florian Luca, Divyum Sharma, On the number of non-zero digits of integers in multi-base representations, Publ. Math. Debrecen 90 (1–2) (2017) 181–194.

[6] Valérie Berthé, Laurent Imbert, Diophantine approximation, Ostrowski numeration and the double-base number system, Discrete Math. Theor. Comput. Sci. 11 (1) (2009) 153–172.

[7] Yann Bugeaud, Effective irrationality measures for quotients of logarithms of rational numbers, Hardy-Ramanujan J. 38 (2015) 45–48.

[8] Parinya Chalermsook, Hiroshi Imai, Vorapong Suppakitpaisarn, Two lower bounds for shortest double-base number system, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E98.A (6) (2015) 1310–1312.

[9] Henri Cohen, Analysis of the sliding window powering algorithm, J. Cryptology 18 (1) (2005) 63–76.

[10] Vassil S. Dimitrov, Everett W. Howe, Lower bounds on the lengths of double-base representations, Proc. Amer. Math. Soc. 139 (10) (2011) 3423–3430.

[11] Vassil Dimitrov, Laurent Imbert, Pradeep K. Mishra, The double-base number system and its application to elliptic curve cryptography, Math. Comp. 77 (262) (2008) 1075–1104.

[12] Vassil S. Dimitrov, Graham A. Jullien, William C. Miller, An algorithm for modular exponentiation, Inform. Process. Lett. 66 (3) (1998) 155–159.

[13] Vassil S. Dimitrov, Graham A. Jullien, William C. Miller, Theory and applications of the double-base number system, IEEE Trans. Comput. 48 (1999) 1098–1106.

[14] Peter J. Grabner, Clemens Heuberger, On the number of optimal base 2 representations of integers, Des. Codes Cryptogr. 40 (1) (2006) 25–39.

[15] Clemens Heuberger, Daniel Krenn, Optimality of the width-w non-adjacent form: General characterisation and the case of imaginary quadratic bases, J. Théor. Nombres Bordeaux 25 (2) (2013) 353–386.

[16] Clemens Heuberger, James A. Muir, Unbalanced digit sets and the closest choice strategy for minimal weight integer representations, Des. Codes Cryptogr. 52 (2009) 185–208.

[17] Daniel Krenn, Dimbinaina Ralaivaosaona, Stephan Wagner, On the number of multi-base representations of an integer, in: 25th International Conference on Probabilistic, Combinatorial, and Asymptotic Methods for the Analysis of Algorithms (AofA'14), DMTCS-HAL Proceedings, Vol. BA, 2014, pp. 229–240.

[18] Daniel Krenn, Dimbinaina Ralaivaosaona, Stephan Wagner, Multi-base representations of integers: asymptotic enumeration and central limit theorems, Appl. Anal. Discrete Math. 9 (2) (2015) 285–312.

[19] Daniel Krenn, Jörg Thuswaldner, Volker Ziegler, On linear combinations of units with bounded coefficients and double-base digit expansions, Monatsh. Math. 171 (3–4) (2013) 377–394.

[20] L. Kuipers, H. Niederreiter, Uniform Distribution of Sequences, Pure and Applied Mathematics, Wiley-Interscience/John Wiley & Sons, New York-London-Sydney, 1974.

[21] Eyal Kushilevitz, Communication complexity, Adv. Comput. 44 (1997) 331–360.

[22] François Morain, Jorge Olivos, Speeding up the computations on an elliptic curve using addition-subtraction chains, RAIRO Theor. Inform. Appl. 24 (1990) 531–543.

[23] James A. Muir, Douglas R. Stinson, Minimality and other properties of the width-w nonadjacent form, Math. Comp. 75 (2006) 369–384.

[24] Braden Phillips, Neil Burgess, Minimal weight digit set conversions, IEEE Trans. Comput. 53 (2004) 666–677.

[25] George W. Reitwiesner, Binary Arithmetic, Advances in Computers, vol. 1, Academic Press, New York, 1960, pp. 231–308.

[26] Jerome A. Solinas, Efficient arithmetic on Koblitz curves, Des. Codes Cryptogr. 19 (2000) 195–249.

[27] Jörg M. Thuswaldner, Summatory functions of digital sums occurring in cryptography, Period. Math. Hungar. 38 (1–2) (1999) 111–130.

[28] Robert Tijdeman, On the maximal distance between integers composed of small primes, Compos. Math. 28 (1974) 159–162.
[29] Andrew Chi-Chih Yao, Some complexity questions related to distributive computing (preliminary report), in: Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing, STOC '79, ACM, New York, NY, USA, 1979, pp. 209–213.
[30] Wei Yu, Kunpeng Wang, Bao Li, Song Tian, On the expansion length of triple-base number systems, in: Amr Youssef, Abderrahmane Nitaj, Aboul Ella Hassanien (Eds.), Progress in Cryptology – AFRICACRYPT 2013, Berlin, Heidelberg, Springer, Berlin Heidelberg, 2013, pp. 424–432.