Lower bounds for the strong n-conjecture*

Aquinas Hobor[1], Rupert Hölzl[2], Elaine Li[3] and Frank Stephan[4 5]

[1] Computer Science, University College London, Gower Street, London WC1E 6BT, United Kingdom
Email: a.hobor@cs.ucl.ac.uk
[2] Institut 1, Fakultät für Informatik, Universität der Bundeswehr München,
Werner-Heisenberg-Weg 39, 85579 Neubiberg, Germany
Email: r@hoelzl.fr
[3] Yale-NUS College, 16 College Avenue West, Singapore 138527, Republic of Singapore
Email: elaine.li@u.yale-nus.edu.sg
[4] Department of Mathematics, National University of Singapore, Singapore 119076, Republic of Singapore
[5] School of Computing, National University of Singapore, Singapore 117417, Republic of Singapore
Email: fstephan@comp.nus.edu.sg

Abstract. The strong n-conjecture is a generalisation of the *abc*-conjecture to arbitrary n where all n numbers have to be coprime. It asks for the limit superior of the qualities of n-tuples summing up to 0. Konyagin showed that for odd $n \geq 5$, this value is at least $3/2$. Later, other authors added the requirement that zero subsums be excluded. We follow their results, even in a slightly stricter way, and show that for odd $n \geq 5$, the limit quality is at least $5/3$ and for even $n \geq 6$, the limit quality is at least $5/4$. This latter result improves a bound of 1 obtained by Browkin. Furthermore, we construct for all $n \geq 6$ and $m \geq 3$ a sequence of n-tuples who do not contain any multiples of $3, 4, \ldots, m$ and whose qualities approach $5/4$. For the Gaussian integers (= complex integers), we show that for $n \geq 4$ the quality is at least $5/3$, again with excluding any given finite set of factors (except that odd n require that one of the Gaussian integers is even).

1 Introduction

The *abc*-conjecture [11, 12, 20] is a well-known open problem in mathematics that postulates that there is no constant $q > 1$ such that for infinitely many tuples (a, b, c) of coprime and nonzero integers with $a + b + c = 0$ the quality $\log(\max\{|a|, |b|, |c|\})/\log(\mathrm{rad}(a \cdot b \cdot c))$ exceeds q. Here $\mathrm{rad}(a \cdot b \cdot c)$ is the largest square-free divisor of $a \cdot b \cdot c$. For example, given a tuple $(8192, -8181, -11) = (2^{13}, -3^4 \cdot 101, -11)$, its entries are pairwise coprime, their largest square-free divisor is $6666 = 2 \cdot 3 \cdot 11 \cdot 101$ and its quality is $\log(8192)/\log(6666)$, which is approximately 1.0234.

The conjecture itself is quite well-studied and still unresolved. On the way towards partial solutions, various variants of it led to new related conjectures being made. While Vojta [18,

* F. Stephan is supported in part by Singapore Ministry of Education Academic Research Fund Tier 2 grants MOE2016-T2-1-019 / R146-000-234-112 and MOE2019-T2-2-121 / R146-000-304-112.

19] has studied a very general statement that implies the *abc*-conjecture, a more immediate generalization is the n-conjecture first studied by Browkin and Brzeziński [2].

Many variants of the n-conjecture are possible and in this article we deal with two such variants introduced by Browkin [1] and Ramaekers [14], respectively. Both authors have called their variants "strong n-conjectures", because they do not only require that the overall set of entries of each n-tuple has no common factor, but that each pair of numbers in the tuple is coprime. They also make additional modifications which have the consequence that their respective versions of the conjecture are incomparable with the n-conjecture. In the rest of this article we will simply refer to their incomparable versions as Browkin's and Ramaekers' conjectures, respectively. Both conjectures concern the possible values of the following quantity.

Definition 1. *For $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ we write*

$$q(a_1, a_2, \ldots, a_n) = \frac{\log(\max\{|a_1|, |a_2|, \ldots, |a_n|\})}{\log \operatorname{rad}(a_1 \cdot a_2 \cdot \ldots \cdot a_n)}$$

where for a number x, $\operatorname{rad}(x)$ is the largest squarefree divisor of x. Then for an infinite set of n-tuples $A = \{a_1, a_2, \ldots\} \subseteq \mathbb{Z}^n$, let the quality of A be defined as

$$Q_A = \limsup_{k \to \infty} q(a_k)$$

where the enumeration $a_1, a_2, \ldots$ of A must be one-one.

Different conjectures arise when considering different sets A and making different predictions about Q_A's value. The main goal of this article is to clarify the relation between these different conjectures and to try to unify the picture. We start by presenting Browkin's and Ramaekers' conjectures and explaining how they differ. We then define our own variant, with two objectives:

First, our version has several parameters, and is therefore a template for obtaining multiple different conjectures to study, which we will do. But secondly, for some choice of those parameters, we obtain a conjecture that is at the same time stronger than both Browkin's and Ramaekers' version. Here stronger means that any lower bound for the quality defined according to us is necessarily also a lower bound for the qualities appearing in both Browkin's and Ramaekers' version.

We then show some lower bounds for quality as defined by us for this particular choice of parameters. For this purpose, we improve a construction of Konyagin (see Browkin [1]) establishing lower bounds for Browkin's quality in such a way that it also establishes lower bounds for our more demanding definition of quality. An immediate corollary will be that Ramaekers' conjecture is false (in fact, this already followed from Konyagin's unmodified result).

Next, we take advantage of the freedom offered by the new parameters that we introduced with our definition. This allows us to apply similar techniques as before to more general questions. One of the requirements in the previously known conjectures was to only consider n-tuples of integers that are pairwise coprime. We loosen this requirement by allowing g.c.d.s to be inside some finite set $E \supseteq \{1\}$. Also, we can restrict the sets of n-tuples considered in the definition

of quality by disallowing all n-tuples containing entries that are multiples of elements of some set F.

We point out that our proof techniques are mostly elementary and often inspired by existing literature in the field. Nonetheless, by modifying them according to our needs, we achieve new and stronger results.

2 Preliminaries

Even though it is not the subject of this article, we first recall the n-conjecture and how it relates to the *abc*-conjecture.

Conjecture 2 (n-conjecture; Browkin and Brzeziński [2]). *Let $n \geq 3$ and let*

$$A(n) = \left\{ (a_1, \ldots, a_n) \in \mathbb{Z}^n \colon \begin{array}{c} a_1 + \ldots + a_n = 0, \ \gcd(a_1, \ldots, a_n) = 1, \text{ and there} \\ \text{are no } b_1, \ldots, b_n \in \{0, 1\} \text{ and } i, j \text{ with } 1 \leq i, j \leq n \\ \text{such that } b_i = 0 \text{ and } b_j = 1 \text{ and } \sum_{k=1}^{n} b_k \cdot a_k = 0 \end{array} \right\}.$$

Then $Q_{A(n)} = 2n - 5$ for every n.

Theorem 3 (Browkin and Brzezinski [2]). *If the abc-conjecture is false then the n-conjecture is false for every $n \geq 4$.*

The first "strong n-conjecture" that we study is the following. It is obtained from the n-conjecture by requiring that the entries in each n-tuple are pairwise coprime and removing the condition that forbids proper subsums of the numbers in the n-tuples to equal 0.

Conjecture 4 (Browkin [1]). *Let $n \geq 3$ and let*

$$B(n) = \left\{ (a_1, \ldots, a_n) \in \mathbb{Z}^n \colon \begin{array}{c} a_1 + \ldots + a_n = 0 \text{ and } \gcd(a_i, a_j) = 1 \\ \text{for } i, j \text{ with } 1 \leq i < j \leq n \end{array} \right\}.$$

Then $Q_{B(n)} < \infty$ for every n.

Note that, if we fix $n = 3$ and replace "$Q_{B(n)} < \infty$" by "$Q_{B(n)} = 1$", we obtain the *abc*-conjecture.

Note also that $Q_{A(4)} = 3$ implies $Q_{B(3)} = 1$. To see this latter point, assume that there are infinitely many counter examples (a, b, c) to the *abc*-conjecture of quality at least q with $q > 1$. Then these examples also witness that $Q_{A(4)} \geq 3q$ via the four-tuples $(a^3, b^3, c^3, -3abc)$. Similarly, for $n = 5$, consider the set of n-tuples of the form $(a^5, b^5, c^5, -5abc^3, 5a^2b^2c)$ which all have quality at least $5q$.

Theorem 5 (Konyagin; see Browkin[6] [1]).

$$Q_{B(n)} \geq \begin{cases} 1 & \text{if } n \geq 4 \text{ is even,} \\ 3/2 & \text{if } n \geq 5 \text{ is odd.} \end{cases}$$

[6] We point out that there is a typo when Browkin states Konyagin's result; where we say "$n \geq 5$" he says "$n \geq 3$". But then Theorem 5 would already disprove the *abc*-conjecture. Indeed, Konyagin's proof only works for odd $n \geq 5$.

The second "strong n-conjecture" that we study is the following.

Conjecture 6 (Ramaekers [14]). *Let $n \geq 3$ and let*

$$R(n) = \left\{ (a_1, \ldots, a_n) \in \mathbb{Z}^n \colon \begin{array}{c} a_1 + \ldots + a_n = 0, \\ \gcd(a_i, a_j) = 1 \text{ for } i, j \text{ with } 1 \leq i < j \leq n, \text{ and there} \\ \text{are no } b_1, \ldots, b_n \in \{0, 1\} \text{ and } i, j \text{ with } 1 \leq i, j \leq n \\ \text{such that } b_i = 0 \text{ and } b_j = 1 \text{ and } \sum_{k=1}^{n} b_k \cdot a_k = 0 \end{array} \right\}.$$

Then $Q_{R(n)} = 1$ for every n.

Note that Ramaekers' conjecture maintains the subsum condition from the original n-conjecture, unlike Browkin's. Furthermore, again unlike Browkin's, Ramaekers' conjecture makes a claim about the exact numerical value of the quality. Darmon and Granville [4, End of Section 5.2] also mention this statement as the "generalised *abc*-conjecture", but only conjecturing $Q_{R(n)} < \infty$ and without clarifying whether they require pairwise or setwise coprimeness.

Except for $(1, -1, 0)$ and its reorderings, all triples in $B(3)$ are also in $R(3)$, thus the *abc*-conjecture is again equivalent to the statement that $Q_{R(3)} = 1$. Ramaekers computed many elements of $R(3)$, $R(4)$ and $R(5)$ with quality larger than 1; however, the qualities of the tuples in $R(4)$ are in general smaller than those of the examples in $R(3)$. Thus it might be that disproving the conjecture $Q_{R(4)} = 1$ is even more challenging than disproving the *abc*-conjecture. We do not know if there is any implication between the cases for $n = 3$ and $n = 4$. For larger n, however, we will see below that $Q_{R(n)} > 1$.

The set $R(n)$ is strictly smaller than the set $B(n)$, so by definition $Q_{R(n)}$ could be smaller than $Q_{B(n)}$. Therefore, a statement analogous to Theorem 5 cannot be trivially inferred to hold for $Q_{R(n)}$. Indeed, for odd $n \geq 7$, Konyagin's proof of Theorem 5 uses n-tuples which are in $B(n) \setminus R(n)$. However, we will show below how it can be amended to correct this "flaw" in order to refute Ramaekers' conjecture. In fact, we will even improve Konyagin's construction to work for the quality appearing in the following open problem. Here we introduce two new parameters, the exception set E and the set of forbidden factors F.

Open Problem 7. *Let $n \geq 3$ and $E, F \subset \mathbb{N}$ be finite sets such that $E \cap F = \emptyset$, $1 \in E$ and $\min F \geq 3$. Also let $U(E, F, n)$ contain all $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ satisfying the following conditions:*

(i) $\gcd(a_i, a_j) \in E$ *for* i, j *with* $1 \leq i < j \leq n$;
(ii) $a_1 + \ldots + a_n = 0$;
(iii) *there are no* $b_1, \ldots, b_n \in \{-1, 0, 1\}$ *and* i, j *with* $1 \leq i, j \leq n$ *such that* $b_i = 0$ *and* $b_j = 1$ *and* $\sum_{k=1}^{n} b_k \cdot a_k = 0$;
(iv) *none of the numbers $a_1, \ldots, a_n$ is a multiple of any number in F.*

Fixing different interesting choices of E, F and n, what are meaningful upper and lower bounds on $Q_{U(E,F,n)}$?

Note that our subsum condition (ii) is more demanding than the ones studied previously as we also allow negative terms in the subsums. Also note how in condition (i) we allow all g.c.d.s from

the set E, instead of only allowing the g.c.d. 1 as in the previous conjectures. We point out that making the set E smaller only makes it harder to establish lower bounds. Thus, whenever we establish a lower bound for the case $E = \{1\}$ in the remainder of the article, that lower bound immediately also holds for larger sets E, and we will often not explicitly mention this fact.

Concerning condition (iv), the set F can be empty, in which case the condition is trivially satisfied by every n-tuple. Furthermore, $(a_1, \ldots, a_n) \in U(E, F, n)$ must contain an even number of even numbers to satisfy (ii). As a result, if n is even and E does not contain even numbers, then no $(a_1, \ldots, a_n) \in U(E, F, n)$ can contain *any* even entries. So if n is even and E does not contain even numbers, we may w.l.o.g. assume that $2 \in F$. Similarly, when $2 \in F$ and n is odd, then $U(E, F, n) = \emptyset$ as the sum of odd many odd numbers cannot be 0.

Fact 8. *We have $Q_{U(\{1\},\emptyset,n)} \leq Q_{R(n)} \leq Q_{B(n)}$ for every n.*

3 Refuting Ramaekers' conjecture

We now modify Konyagin's construction in the way described above.

Theorem 9 (Konyagin [1]). $Q_{U(\{1\},\emptyset,5)} \geq 3/2$.

Theorem 9 and Fact 8 immediately imply the following corollary.

Corollary 10. *Conjecture 6 is false.*

Proof (Theorem 9). Fix some arbitrary $k \geq 1$ and let $a = (6^{2^k} + 1)^3$, $b = -(6^{2^k} - 1)^3$, $c = -6 \cdot (6^{2^k})^2$, $d = -31$ and $e = 29$. Then $\log(a) \geq 3 \cdot 2^k \cdot \log(6)$, $\mathrm{rad}(a \cdot b \cdot c \cdot d \cdot e)$ is a factor of $(6^{2^k} + 1) \cdot (6^{2^k} - 1) \cdot 6 \cdot 31 \cdot 29$ and its logarithm is bounded by a constant ℓ plus $\log(6) \cdot 2 \cdot 2^k$. Then

$$q(a, b, c, d, e) \geq \frac{3 \cdot 2^k \cdot \log(6)}{2 \cdot 2^k \cdot \log(6) + \ell},$$

which converges to $3/2$ for $k \to \infty$.

We prove that for every $k \geq 1$, if a, b, c, d, e are chosen as above, they are pairwise coprime: The numbers a, b, c are of the forms $(s+1)^3$, $(s-1)^3$ and $-6s^2$, respectively, for $s = 6^{2^k}$. Note that $s-1$ and s are trivially coprime, and that the same holds for s and $s+1$. As 2 and 3 are the only factors of s, neither of them can be a factor of $s-1$ or $s+1$, and thus $(s+1)^3$ and $6s^2$, as well as $(s-1)^3$ and $6s^2$, are coprime. To see that $(s-1)^3$ and $(s+1)^3$ are coprime as well, note that $s-1$ and $s+1$ are both odd, meaning that 2 cannot be a common factor; therefore $s-1$ and $s+1$ are coprime. Then $(s-1)^3$ and $(s+1)^3$ are coprime as well. Finally, we study the sequence $(6^{2^k})_{k \geq 1}$. If we can show that modulo 29 and modulo 31 none of its elements equals -1, 0, or 1, then we have shown that $s-1, s, s+1$ are not multiples of 29 or 31; and thus that each of a, b, c is coprime with both $d = 29$ and $e = 31$. To see this we proceed by repeated squaring: First, modulo 29, we obtain the sequence 6, $6^2 = 36 \equiv 7$, $6^4 \equiv 7^2 = 49 \equiv -9$, $6^8 \equiv (-9)^2 = 81 \equiv -6$, $6^{16} \equiv (-6)^2 = 36 \equiv 7$, and so on. Similarly, modulo 31, we obtain the sequence 6, 5, -6, 5, and so on. Thus, a, b, c, d, e are pairwise coprime, establishing condition (i) in Open Problem 7.

Condition (ii) is immediate. For the subsum condition (iii), choose k large enough. Then if $\pm(s+1)^3$ is part of a subsum, so must $\mp(s-1)^3$ in order to have any hope of achieving a subsum equaling 0; the same holds vice versa. Also, the signs of these two numbers must be opposite; w.l.o.g. assume that they are chosen in such a way that the sum of the two numbers is positive, namely that it equals $6 \cdot s^2 + 2$. Since k was chosen large, we can again argue that $-6s^2$ must be part of the subsum in order to have any hope of achieving a subsum equaling 0. But $(s+1)^3 - (s-1)^3 - 6s^2 = 2$, and thus the only way to achieve a sum of 0 in this case is by also adding 29 and -31. But then all five numbers a, b, c, d, e have been selected for the sum and it is not a proper subsum.

So assume that neither $\pm(s+1)^3$ nor $\mp(s-1)^3$ are part of a subsum. If $\pm 6 \cdot s^2$ is part of a subsum then adding or subtracting 29 or 31 is not enough to achieve a subsum equaling 0 for large enough k. If, on the other hand, $\pm 6 \cdot s^2$ is not part of the subsum either, then using only 29 and 31, a subsum of 0 can clearly not be achieved. □

We mention that Konyagin's result can also be derived from an example given by Darmon and Granville [4, item (d) on page 542] by choosing $t = 2^k$; they cite correspondence with Noam D. Elkies as the source.

For the next result we use a proof that is similar to the last, except that we use a fifth degree polynomial instead of a third degree one to obtain a better bound. In addition we can avoid the factor 3 but not the factors $2, 5, 7, 10$. We point out that the result is closely related to Ramaekers' [14, Section 4.4] that $Q_{U(\{1,2\},\emptyset,4)} \geq 5/3$. He credits the already mentioned examples from Darmon and Granville [4] and Elkies that show that $Q_{U(\{1,2\},\emptyset,4)} > 1$ with the idea of using polynomial identities. The two constants 1 and 7 in the following construction are obtained by splitting the single constant 8 of Ramaekers.

Theorem 11. *Let F be such that $2, 5, 7, 10 \notin F$. Then $Q_{U(\{1\},F,5)} \geq 5/3$.*

Proof. Let $z > \max(F \cup \{11\})$ and $y = z!$. Choose a large enough k and x such that $x + 1 = (y+1)^k$. Note that x is a multiple of y, as $x = (y+1)^k - 1 = \sum_{h=1}^{k} \binom{k}{h} \cdot y^h$. Then consider $a = (x+1)^5$, $b = -(x-1)^5$, $c = -10 \cdot (x^2+1)^2$, $d = 7$ and $e = 1$.

Condition (i) in Open Problem 7 holds for every such a, b, c, d, e for reasons analogous to those in the proof of Theorem 9, together with the observation that, as x is a multiple of 7, none of a, b, c can be a multiple of 7.

Condition (ii) is satisfied, as $a+b+c+d+e = 10x^4 + 20x^2 + 2 + c + d + e = -8 + d + e = 0$.

For condition (iii), first note that since the residues of a, b, c, d, e modulo 20 — which is a factor of y — are 1, 1, 10, 7 and 1, respectively, we have that if c or d are part of a subsum then so must all of a, b, c, d, e. The only subsums without c and d that we need to consider are $a - b$ or $a - e$ or $b - e$ or $a - b - e$, but these equal $(x+1)^5 - (x-1)^5$, $(x+1)^5 - 1$, $(x-1)^5 - 1$ and $(x-1)^5 - 2$, respectively, and as we chose $k \geq 1$ and $x \geq 11!$ none of them can equal 0.

As x is a multiple of y, every number in $\{2, 3, \ldots, z\} \supseteq F$ divides x, and therefore no such number divides any of $x - 1, x + 1, x^2 + 1$. Similarly, no number in F divides $10 \cdot (x^2+1)^2$. Consequently, none of a, b, c, d, e is a multiple of any element of F, which establishes condition (iv).

The quality lower bound of $5/3$ in the limit can be established by modifying the argument from the proof of Theorem 9 in the obvious way. □

The following proposition will be useful for later arguments.

Proposition 12. *Let $u, m \in \mathbb{N}$ with $m \geq u$, $q = \prod_{p \leq m \wedge p \text{ prime}} p$ and $F = \{3, 4, \ldots, m\}$. Then there are a natural number v and an integer w with $u = v + w$ such that no element of F divides v or w, $\gcd(v, w) = 1$ and $q \leq v \leq |w| \leq (m + 1) \cdot q$.*

Proof. Let q be as in the statement. We run the following algorithm:

(1) Let $v = u + 1 + q$ and $w = -q - 1$.
(2) For all prime numbers $3 \leq p \leq m$,
(3) while p divides one of v or w,
(4) let $v = v + q/p$ and $w = w - q/p$.
(5) If 4 divides v then let $v = v + q$ and $w = w - q$.

Note that the sum $v + w = u$ and the fact that w is odd are invariants during the execution of this algorithm. Further note that $q \leq v$ and $|w| \leq (m + 1) \cdot q$ are immediate by construction.

During the "for" loop over p, since q/p is not a multiple of p, only one of the numbers v, $v + q/p$, $v + q/p + q/p$ can be a multiple of p. The same applies to the numbers w, $w - q/p$, and $w - q/p - q/p$. Thus, for each p, the instruction inside the "while" loop will be executed 0, 1 or 2 times, and afterwards neither v nor w will be divisible by p.

We claim that, once established, this property is preserved throughout the rest of the algorithm: Consider some prime $p' \neq p$ which was handled in a previous iteration of the "while" loop, and assume that at the beginning of the iteration for p of the "while" loop we have that neither v nor w are divisible by p'. Since q/p is a multiple of p', we have $v \equiv v + q/p \pmod{p'}$ and $w \equiv w - q/p \pmod{p'}$; thus the property is preserved by the action of line (4). For similar reasons, the property also is preserved during the final execution of line (5). This proves the claim, and it follows that after the algorithm terminates, v and w are not divisible by any odd prime $\leq m$.

Assume that v is divisible by 4 before the execution of line (5). Then, since q is not divisible by 4, $v + q$ is an even number *not* divisible by 4. Thus, in any case, after the execution of line (5), v is not divisible by 4. Since w was odd, it is still odd after the execution of line (5); in particular it is not divisible by 4.

Overall we have established that, when the algorithm terminates, none of the numbers $3, 4, \ldots, m$ divide v or w.

To see that v and w are coprime, first note that 2 cannot be a common prime factor since w is odd. By construction, any odd common prime factor p of v and w must be larger than m. But any such p also is a prime factor of $u = v + w$, which is impossible as $u \leq m$. □

The following result, which to the best of our knowledge is new,[7] shows that Ramaekers' conjecture can be refuted for any even $n \geq 6$, even with arbitrary forbidden set F.

[7] In 2000, Browkin [1] stated that nothing is known about this case.

Theorem 13. *Let F be arbitrary and let $n \geq 6$. Then $Q_{U(\{1\},F,n)} \geq 5/4$.*

In the proof, we will use the following well-known fact.

Theorem 14 (Dirichlet's Prime Number Theorem [5]). *For every two positive coprime integers a and d, there are infinitely many positive integers n such that $a + nd$ is prime.*

Proof (Theorem 13). As enlarging F only makes the statement harder to prove, we can assume that $F = \{3, 4, \ldots, \ell\}$ for some $\ell \geq 11$.

Let $s = \ell!$. By Theorem 14, there are infinitely many positive integers t such that $10 \cdot s \cdot t - 1$ is prime. Choose such a t with $t > 101$ and let $y = s \cdot t$. Since $10 \cdot y - 1$ is prime and larger than $y + 1$, it is clear that these two numbers are coprime. Then there are infinitely many positive integers h such that $(y+1)^h \equiv 1 \pmod{10 \cdot y - 1}$, and for such h we have in particular that $(y+1)^{h!} \equiv 1 \pmod{10 \cdot y - 1}$. Later, we will let h go to infinity, but for the moment we give an analysis that is true independently of the exact value of h as long as h is large enough.

So let x be $(y+1)^{h!}$. First note that since y is even, x is odd by definition. Secondly, if we expand the product in the definition of x, we obtain a polynomial in y with constant term 1; in this polynomial, each of the non-constant terms is divisible by y and therefore by every element of F. Then, the presence of the constant term 1 in the polynomial implies that $\gcd(x, y) = 1$ and in particular that x is not divisible by any element of $F \cup \{2\}$. (†)

We choose the first four entries of the n-tuple $(a_1, \ldots, a_n)$ as follows:

- $a_1 = (x + y)^5$;
- $a_2 = -(x - y)^5$;
- $a_3 = -(10y - 1) \cdot x^4$;
- $a_4 = -(x^2 + 10y^3)^2$.

Of course we haven't fixed h yet, so that the exact value of x is not yet determined, and the same is consequently true for $a_1, \ldots, a_n$. However, we can already observe that

$$a_1 + a_2 + a_3 + a_4 = -2y^5 + 100y^6 \qquad (‡)$$

and therefore that $a_1 + a_2 + a_3 + a_4$ is independent of x. We continue with the definition of $a_7, a_8, \ldots, a_n$ in a way that does not depend on x.

- Choose $a_7, a_8, \ldots, a_n$ as negated odd prime numbers such that $|a_7| > 700y^6$ and such that for $k = 7, 8, \ldots, n-1$ we have $6 \cdot |a_k| < |a_{k+1}|$.

Finally, we choose the remaining two elements a_5 and a_6; by the preceding choices and arguments the following definition is independent of x.

- Let u be such that $u + a_1 + a_2 + a_3 + a_4 + (\sum_{k=7}^{n} a_n) = 0$ and let $m = 4u$. By the previous choices, it is easy to see that u must be a positive number. So we can apply Proposition 12 to these values of u and m and let a_5 and a_6 be the numbers v and w with $u = v + w$ as provided by that proposition.

We will show in a moment that, for every h chosen large enough, all four conditions in Open Problem 7 are met by $(a_1, \ldots, a_n)$. We claim that this implies that $Q(E, F, n) \geq 5/4$. To see that, note that $\mathrm{rad}(a_1 \cdot \ldots \cdot a_n)$ will be a divisor of

$$(x + y) \cdot (x - y) \cdot (10y - 1) \cdot (x^2 + 10y^3) \cdot a_5 \cdot \ldots \cdot a_n.$$

Letting h go to infinity does not affect $a_5, \ldots, a_n$ and inside the other terms in the above expression only x grows with h while all other parts remain constant. Thus, $\mathrm{rad}(a_1 \cdot \ldots \cdot a_n)$ is bounded from above by a polynomial in x of degree at most 4, while, due to the choice of a_1, $\max\{|a_1|, |a_2|, \ldots, |a_n|\}$ is bounded from below by a polynomial in x of degree 5. Using L'Hôpital's rule and the chain rule, $Q(E, F, n) \geq 5/4$.

It remains to show that for all h large enough, all four conditions in Open Problem 7 are met by $(a_1, \ldots, a_n)$. That condition (ii) holds is immediate by how we chose a_5 and a_6.

By an analogous argument to that used for (†), it can be seen that each of a_1, a_2, a_3, a_4 equals 1 modulo any prime factor of y, thus is not divisible by any element of F. The same is true by construction for each of $a_5, \ldots, a_n$. It follows that condition (iv) ist met.

Next, we establish condition (i) in several intermediate steps:

- *a_1 and a_2 are coprime:* Note that any common prime divider of a_1 and a_2 must also be a factor of $2y$, as it must divide $x+y$ and $x-y$ and thus their difference. Note that y is even by construction, so that y has the same prime dividers as $2y$. Thus, any common prime divider of a_1 and a_2 must also divide y and, consequently, x. But we already know that $\gcd(x, y) = 1$.
- *a_3 is coprime with both a_1 and a_2:* The factor x of a_3 is coprime with $x + y$ and $x - y$, as x is coprime to y. Furthermore, $x = (y + 1)^{h!} \equiv 1 \pmod{10y - 1}$ and thus

  $$x + y \equiv 1 + y \not\equiv 0 \pmod{10y - 1} \quad \text{and} \quad x - y \equiv -y + 1 \not\equiv 0 \pmod{10y - 1}.$$

  Consequently, $10y-1$ divides neither $x+y$ nor $x-y$ and, together with the fact that $10y-1$ is prime, we obtain that a_3 is coprime with a_1 and a_2.
- *a_3 and a_4 are coprime:* We establish this by showing that a_4 is coprime with both factors of a_3. First, to determine $\gcd(10y - 1, a_4)$, note that $x^2 \equiv 1 \pmod{10y - 1}$. Observe that

  $$100y^2 - 1 = (10y - 1) \cdot (10y + 1) \equiv 0 \pmod{10y - 1},$$

  which implies $y^2 + 1 \equiv 101y^2 \pmod{10y - 1}$. Thus

  $$x^2 + 10y^3 \equiv 1 + 10y^3 \equiv (10y - 1) \cdot y^2 + y^2 + 1 \equiv 101y^2 \pmod{10y - 1}.$$

  Trivially, the primes 101 and $10y - 1 > 101$ have no common factor. And any common factor of y^2 with $10y - 1$ would also have to be a factor of y, thus of $10y$, thus of 1. As a result, $\gcd(10y - 1, a_4) = 1$.
  Secondly, we must determine $\gcd(x, a_4) = \gcd(x, x^2 + 10y^3)$. Clearly, this number must divide $10y^3$. But by (†), no divider of y nor any element of $F \cup \{2\}$ divides x. Therefore, $\gcd(x, a_4) = 1$.

- *a_4 is coprime with both a_1 and a_2:* Clearly, $a_1 \cdot a_2$ is a power of $(x+y)(x-y) = x^2 - y^2$ and a_4 is a (negated) power of $x^2 + 10y^3$. Any common prime factor p of a_4 with either a_1 or a_2 would therefore have to be a factor of the difference between the previous two expressions, thus of $10y^3 + y^2 = y^2 \cdot (10y+1)$. Such a p divides one of $x+y$ or $x-y$; thus, it cannot be a factor of y, because otherwise it would divide x, contradicting the coprimeness of x and y. Thus, such a p would have to be a prime factor of $10y+1$. Recall that $x \equiv 1 \pmod{10y+1}$, thus in particular $x \equiv 1 \pmod{p}$. Since p divides one of $x+y$ or $x-y$, it would also be a prime factor of either $(10y+1) - 10 \cdot (x+y) = -10x + 1 \equiv -9 \pmod{p}$ or of $(10y+1) + 10 \cdot (x-y) = 10x + 1 \equiv 11 \pmod{p}$. This can only be true if $p \in \{3, 11\}$, which is impossible since both 3 and 11 divide y and thus cannot divide $10y+1$. In conclusion, a_4 is coprime with both a_1 and a_2.
- *Each of a_1, a_2, a_3 is coprime with each of $a_5, \ldots, a_n$:* If h is chosen large enough, then by construction, a_5 and a_6 only have prime factors between $m > |a_7| > 700y^6$ and h. Observe that for any prime p with $y+1 < m < p \leq h$ it holds that $p-1$ divides $h!$, and thus, by Fermat's Little Theorem, $x = (y+1)^{h!} \equiv 1 \pmod{p}$. This holds in particular for any prime p dividing a_5 or a_6 and for all primes $p \in \{a_7, a_8, \ldots, a_n\}$; thus any such p is coprime with x. Since for such a p we also have $p > 700y^6$ by construction, it follows that p is coprime with $x+y$ and $x-y$ as well. As we trivially have $p \neq 10y-1$, we can conclude that p does not divide any of a_1, a_2, a_3.
- *a_4 is coprime with each of $a_5, \ldots, a_n$:* For the same reasons as in the previous item, we only need to consider potential prime factors p between $700y^6$ and h. For such p, we again have that $x \equiv 1 \pmod{p}$ by the choice of x. Then $x^2 + 10y^3 \equiv 1 + 10y^3 \not\equiv 0 \pmod{p}$, which implies that p does not divide a_4.
- *$a_5, \ldots, a_n$ are pairwise coprime:* First, being pairwise distinct primes, the $a_7, a_8 \ldots, a_n$ are trivially pairwise coprime. Secondly, recall how a_5 and a_6 were defined using Proposition 12 in such a way as to ensure that a_5 and a_6 are coprime with each other. Finally, the proposition also guarantees that no primes less than m divide a_5 or a_6; as m is larger than any of $|a_i|$ for $7 \leq i \leq n$, we have in particular that both of a_5 and a_6 are coprime with each of $a_7, a_8 \ldots, a_n$.

It remains to establish the subsum condition (iii) for $(a_1, \ldots, a_n)$ via a series of claims. In the following, let $b_1, b_2, \ldots, b_n \in \{-1, 0, +1\}$ be such that $\sum_{k=1}^{n} b_k \cdot a_k = 0$.

- *It must hold that $b_1 = b_2 = b_3 = b_4$:* Recall that the $a_5, \ldots, a_n$ do not depend on x. Since $x = (y+1)^{h!}$, this implies for h large enough that $x > 100 \cdot (|a_5| + |a_6| + \ldots + |a_n|)$. Thus, if for some choice of (b_1, b_2, b_3, b_4) we have that $|\sum_{k=1}^{4} b_k \cdot a_k| > x$, then *no* choice of $(b_5, b_6, \ldots, b_n)$ can lead to $\sum_{k=1}^{n} b_k \cdot a_k = 0$. We will argue that this must be the case unless we have $b_1 = b_2 = b_3 = b_4$.
  So let us inspect all possible choices of (b_1, b_2, b_3, b_4). We first exclude some trivial cases: First, if only one of b_1, b_2, b_3, b_4 is non-zero, then clearly $|\sum_{k=1}^{4} b_k \cdot a_k| > x$. Secondly, the fact that a_1 has positive sign while a_2, a_3, a_4 have negative sign means that for some choices of (b_1, b_2, b_3, b_4) we have $|\sum_{k=1}^{4} b_k \cdot a_k| > x$ simply because either all summands are positive or all are negative; we omit these cases. Finally, to reduce further the numbers of cases to

inspect, we assume w.l.o.g. that $b_i = 1$ when $1 \leq i \leq 4$ is smallest such that $b_i \neq 0$; the case $b_i = -1$ is symmetric. Then the remaining cases that do not have $b_1 = b_2 = b_3 = b_4$ are
- $a_1 + a_2 + b_3 \cdot a_4 + b_4 \cdot a_4$ where $(b_3, b_4) \neq (1, 1)$,
- $a_1 - a_2 + b_3 \cdot a_4 + b_4 \cdot a_4$,
- $a_1 + b_3 \cdot a_3 + b_4 \cdot a_4$,
- $a_2 + b_3 \cdot a_3 + b_4 \cdot a_4$,
- $a_3 + b_4 \cdot a_4$,

and all of them clearly have absolute values that are lower-bounded by x. Thus, the only remaining cases are those where $b_1 = b_2 = b_3 = b_4$.

With this property established, we can from now on treat $a_1 + \cdots + a_4$ as a *single* number that can either be part of a subsum or not.

- *It must hold that $b_5 = b_6$:* Note that by the choice of a_5 and a_6 and by the properties ensured by Proposition 12 we have that $a_5 > 0$ and $a_6 < 0$ and that

$$a_5, |a_6| > (|a_1| + |a_2| + |a_3| + |a_4|) + \sum_{k=7}^{n} |a_n|.$$

  Thus, in any zero subsum, a_5 and a_6 must either not occur at all or in such a way that they partly cancel each other out additively. This is only possible when $b_5 = b_6$.

Again, from now on we treat $a_5 + a_6$ as a *single* number that may be part of a subsum or not. To complete the proof we distinguish all three possible cases concerning the value of $b_5 = b_6$.

- *If $b_5 = b_6 = 0$, then the subsum is empty:* This is because in the sequence

$$|a_1 + a_2 + a_3 + a_4|, |a_7|, |a_8|, \ldots, |a_n|$$

  each entry is more than 6 times the previous one; so that the only way of obtaining a zero subsum in the case $b_5 = b_6 = 0$ is by letting $b_k = 0$ for all $1 \leq k \leq n$.
- *If $b_5 = b_6 = 1$, then $b_k = 1$ for all $1 \leq k \leq n$:* Assume that for some choice of $(b_k)_{1 \leq k \leq n}$ with $b_5 = b_6 = 1$ we have $\sum_{k=1}^{n} b_k \cdot a_k = 0$. Since we also have $\sum_{k=1}^{n} a_k = 0$ it follows that

$$\sum_{k=1}^{n} a_k - \sum_{k=1}^{n} b_k \cdot a_k = (1 - b_1) \cdot (a_1 + a_2 + a_3 + a_4) + \sum_{k=7}^{n} (1 - b_k) \cdot a_k = 0,$$

  where $1 - b_k \in \{0, 1, 2\}$ for $k \in \{1, 7, 8, \ldots, n\}$. For the same reason as in the previous item, the only choice of $(1 - b_k)_{k \in \{1,7,8,\ldots,n\}}$ that makes this equality true is $1 - b_k = 0$ (thus $b_k = 1$) for all $k \in \{1, 7, 8, \ldots, n\}$.
- *If $b_5 = b_6 = -1$, then $b_k = -1$ for all $1 \leq k \leq n$:* This is shown by a symmetric argument.

Thus condition (iii) holds, completing the proof. □

We can obtain the following corollary by adapting the proof of Theorem 11 for the case $n = 5$ and the proof of Theorem 13 for the case $n \geq 6$. The details are left to the reader.

Corollary 15. *If $n \geq 5$ is odd and $F \subseteq \{3, 4, \ldots, m\}$ does not contain any multiple of 2 or 5 then $Q_{U(\{1\},F,n)} \geq 5/3$.*

Next, we prove the following theorem.

Theorem 16. *Let F be a finite set with $\min(F) \geq 3$. Then $Q_{U(\{1\},F,5)} > 1$.*

We point out that, to prove this statement, the approaches of Theorems 9 and 11 will not work, as the use of binomial formulas there had the effect that one of the entries of the constructed 5-tuples are divisible by 3 or 5. The technique used in the proof of Theorem 13 is not applicable either, as the splitting of one term into two via Proposition 12 can only be carried out for n-tuples with $n \geq 6$. We thus require a new argument.

Proof. As before, we can assume that $F = \{3, 4, 5, \ldots, m\}$ for some m. Let $p = h! - 1$ for $h > 9m$ and keep h and p constant during the remainder of the construction. Let $x = k!$ in dependency on some sufficiently large parameter $k > p$; as in the previous constructions, we will show that for sufficiently large k all required properties are ensured. Then we will let k go to infinity to obtain infinitely many examples that witness a lower bound for $Q_{U(\{1\},F,5)}$.

Consider the following numbers. The choice of a_1, a_2, a_3 and $a_4 + a_5$ follows Ramaekers [14, Section 4.4]. As in the previous construction, the fourth number is then split into two summands:

- $a_1 = (x + 1)^p$;
- $a_2 = -(x - 1)^p$;
- $a_3 = -2p \cdot (x^2 + (p - 2)/3)^{(p-1)/2}$;
- $a_4 = -(a_1 + a_2 + a_3 + y)$ for some odd number $y > p$ to be chosen below;
- $a_5 = y$.

Note that, as a polynomial in x, $a_1 + a_2$ is of degree $p - 1$ and *even*, that is, of the form $c_0 + c_2x^2 + c_4x^4 + c_6x^6 + \ldots$ Also note that $a_1 + a_2 + a_3$ is an even polynomial in x of degree $p - 5$. Finally note that, when dividing an even polynomial by a polynomial of the form $x^2 + c$, for $c \in \mathbb{Z}$, then the remainder is an integer. Thus, modulo x^2, modulo $x^2 - 1$ and modulo $x^2 + (p - 2)/3$, we have that $a_1 + a_2 + a_3$ is congruent to three integers z_0, z_1 and z_2, respectively. We choose y such that

- none of y, $y + z_0$, $y + z_1$, $y + z_2$ has a prime factor q with $5 \leq q \leq (2p)^p + |z_0| + |z_1| + |z_2|$,
- neither y nor $y + z_0$ are divisible by 2 or 3.

We achieve this by a process that is similar to the one used in the proof of Proposition 12. Let $r = \prod_{q \leq (2p)^p + |z_0| + |z_1| + |z_2| \wedge q \text{ prime}}$ and proceed as follows.

(1) Let $y = 1$.
(2) For all primes q with $5 \leq q \leq (2p)^p + |z_0| + |z_1| + |z_2|$,
(3) let $y = \min(\{y + i \cdot r/q \colon 0 \leq i \leq 4\} \cap \{y' \colon q \nmid y' \wedge q \nmid y' + z_0 \wedge q \nmid y' + z_1 \wedge q \nmid y' + z_2\})$.

Note that q does not divide r/q, and thus, for each $z \in \{y, y + z_0, y + z_1, y + z_2\}$, at most one among $z, z + r/q, \ldots, z + 4 \cdot r/q$ can be a multiple of q. Thus, by the pigeonhole principle, the

choice of y in (3) is always possible. That the final y emerging from this process has the first of the two stipulated properties then follows from an argument analogous to that used in the proof of Proposition 12.

To argue that y has the second property, we first claim that z_0 is divisible by 6. An easy calculation shows that $z_0 = 2 - 2p \cdot ((p-2)/3)^{(p-1)/2}$, an even number. To see that $z_0 \equiv 0 \pmod 3$, it is enough to show that $2p \cdot ((p-2)/3)^{(p-1)/2} \equiv 2 \pmod 3$. For that, note that, as $h! \equiv 0 \pmod 4$, we have that $p - 1 = h! - 2 \equiv 2 \pmod 4$, and thus that $(p-1)/2$ is odd. Recall that $p = h! - 1$, thus $p \equiv 8 \pmod 9$. Now $p - 2 \equiv 6 \pmod 9$ and $(p-2)/3 \equiv 2 \pmod 3$. Now, $(p-2)/3 \equiv p \equiv 2 \pmod 3$ So $2p \cdot ((p-2)/3)^{(p-1)/2} \equiv 2 \pmod 3$ as it is a product of an odd number of factors all of which are congruent to 2 modulo 3. Thus, $z_0 \equiv 0 \pmod 6$, and after the execution of line (1) of the algorithm, $y \equiv y + z_0 \equiv 1 \pmod 6$. As all terms r/q appearing in the algorithm are multiples of 6, this last property is invariant during the algorithm's execution, and the final y and $y + z_0$ are not divisible by 2 or 3, either.

With y chosen, we can now begin to verify properties (i)–(iv) stipulated in Open Problem 7.

Now note that x will be a multiple of 3 due to the choice of the corresponding factorial and that $(p-2)/3$ and p are not multiples of 3, due to $p + 1$ being a multiple of 9, for that reason a_3 is also not a multiple of 3. Furthermore, $2p(x^2 - (p-2)/3)^{(p-1)/2}$ is not divisible by 4, as p is odd, x is even, $p + 1$ is a multiple of 12 and $(p-2)/3$ modulo 6 is either 1 or 3 or 5. Taking into account that all odd prime factors q of members of F divide x and that $p, (p-2)/3$ are not multiples of q, the numbers $x + 1$, $x - 1$ and $x^2 - (p-2)/3$ are not multiples of q. Furthermore, it had been shown above that also $y + z_0$ is not a multiple of q. So none of a_1, a_2, a_3, a_4, a_5 is the multiple of a member of F and condition (iv) is satisfied.

Recall that the properties of this theorem where to be shown for all sufficiently large k only and that $x = k!$; here sufficiently implies in particular that $k \geq 2p + |y| + |z_0 + y| + |z_1 + y| + |z_2 + y|$ and every prime factor of these numbers is a factor of x. Furthermore, any prime factor q of $y, z_0 + y, z_1 + y, z_2 + y$ is neither a factor of $2p$ nor of $(p-2)/3$; thus q is not a factor of a_1, a_2 or a_3, in particular a_1, a_2, a_3 are all three coprime to a_5. Furthermore, if q divides one of a_1 or a_2 then q must also divide $x^2 - 1$ and the remainder of a_4 by $x^2 - 1$ is $z_0 + y$. Thus if q would also divide a_4 then q must divide $z_0 + y$ and that was previously excluded. Similarly, if q divides a_3 and a_4 then q must divide $x^2 + (p-2)/3$ and thus q must be a factor of $z_2 + y$ what was previously excluded.

Furthermore, every prime factor of a_5 will be a factor of x and as a_4 modulo x equals to $2p \cdot (p-2)/3)^{(p-1)/2}$, the common prime factors must be a factor of the latter. But these had been excluded above from being a factor of a_4. Thus a_4 and a_5 are coprime. a_1 and a_2 are coprime, as x is even and thus $x-1$ and $x+1$ are coprime. We have that $(x^2+(p-2)/3)-(x^2-1) = (p-5)/3$. So all the common factors of $x+1$ or $x-1$ on one side and a_3 on the other side are either factors of $2p$ or factors of $(p-5)/3$. As $k > 3p$, these numbers are factors of x and thus not factors of either $x + 1$ or $x - 1$. So a_3 is coprime to both a_1 and a_2. Thus condition (i) is satisfied.

Condition (ii) is also satisfied, by the way the numbers are chosen. Condition (iii) is satisfied, as again one can look at a_1, a_2, a_3, a_4 as polynomials in x and a subsum can only be 0 when these polynomials eliminate all terms depending on x. a_1 and a_2 have degree p and need to be

added in order to obtain degree $p-1$, this needs a_3 to be added in order to get a lower degree; the resulting degree of $p-5$ is the degree of a_4 and that can only be brought to down to the constant y by adding a_4 as well. The constant y needs to be added in order to get 0. These degree arguments work for all sufficiently large k and $x = k!$.

Furthermore, one can see from the degree arguments that $\mathrm{rad}(a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5)$ has, in dependence of x, has the upper size bound $(x^2-1) \cdot (x^2 + (p-2)/3) \cdot O(x^{p-5}) \cdot y$ which is a polynomial of degree $p-1$ using that y is constant but x can be any $k!$ for sufficiently large k. Thus one can esitmate that for $k \to \infty$ the quality is bounded by

$$p \cdot \log(x+1) / \log((x^2-1) \cdot (x^2 + (p-2)/3) \cdot O(x^{p-5}) \cdot y)$$

which is similar to

$$p \cdot \log(x) / \log(x^4 \cdot x^{p-5} \cdot O(1))$$

and thus, one can argue that $Q_{U(\{1\},F,5)} \geq p/(p-1) > 1$. This completes the proof. □

Note that the reason why we can only obtain the strict lower bound 1 using the technique just described is that the value of the ratio $p/(p-1)$ heavily depends on the choice of F.

4 The Role of the Exception Set

Note that we set the requirement that exception sets E have to be finite. The reason is that otherwise certain choices like $E = \{2^h, 2^h+1 : h \in \mathbb{N}\}$ would, for example, allow the tuples $((2^h+1)^3, -2^{3h}, -3 \cdot 2^h \cdot (2^h+1), -1)$ for all $h \in \mathbb{N}$ which would give the same lower bound for $Q_{U(E,\emptyset,4)}$ as the 4-conjecture, assuming that still all numbers as a set should be coprime. If one does also not assume the latter, then for the just chosen E one would even have $Q_{U(E,\emptyset,3)} = \infty$. For finite sets E, the set-wise coprime requirement is not stated, as the value $Q_{U(E,F,n)}$ does not depend on whether the set-wise coprimeness condition is required.

Davies (see Browkin [1]) provides a construction showing that $Q_{U(\{1,2\},\emptyset,4)} \geq 3/2$ and Ramaekers [14, Section 4.4], citing Pomerance [13], discusses a construction giving the better lower bound $Q_{U(\{1,2,4,8\},\emptyset,4)} \geq 5/3$. We state the latter result in the framework of our paper. Note how it contrasts with Ramaekers' conjecture that $Q_{R(4)} = 1$; this demonstrates that just adding 2 into E is a game changer.

Theorem 17. *If $F \subset \mathbb{N}$ is finite such that $2,4,5,8,10 \notin F$, then $Q_{U(\{1,2\},F,4)} \geq 5/3$.*

Proof. Witnessed by the family (depending on k) of numbers $a_1 = (x+1)^5$, $a_2 = -(x-1)^5$, $a_3 = -10 \cdot (x^2+1)^2$ and $a_4 = 8$ with y being the product of all members of $F \cup \{2,3,5,7\}$ and $x = (y+1)^k - 1$ with $k \in \{2,3,\ldots\}$.

As all members of $F \cup \{2,3,5,7\}$ divide x, all members of this set are coprime to $x-1, x+1$ and x^2+1. Thus the only factors of a_1, a_2, a_3, a_4 which can occur in F are those of 10 and 8 which are explicitly excluded from F. Thus condition (iv) is satisfied.

Furthermore, $x-1$ and $x+1$ are coprime, as they are odd; x^2-1 and $10\cdot(x^2+1)$ are also coprime, as x^2 is a multiple of $2\cdot 3\cdot 5$. The greatest common divisor of $-10\cdot(x^2+1)^2$ and 8 is 2 which is a member of the exception set. So condition (i) is satisfied.

Condition (ii) is obtained by simply forming $a_1+a_2+a_3+a_4$ for arbitary x; the resulting polynomial in x vanishes.

Now one looks at possible subsums. It is easy to see that $(x+1)^5$ and $(x-1)^5$ have to be subtracted from each other in order to get a polynomial in x of degree 4 or less; only such a polynomial has a chance to be made to 0 when adding or subtracting the other two terms. When considering sums or subsums of the first three terms, only in two cases the terms depending on x disappear from the sum, namely in the cases $a_1-a_2-a_3$ or $-a_1+a_2+a_3$. The result is either a_4 or $-a_4$. Furthermore, as $x\geq 210$, none of the subsums $a_3, a_4, a_3+a_4, a_3-a_4$ is 0. So condition (iii) is satisfied as well.

As also in previous calculations, one shows that these examples verify that $Q(\{1,2\},F,n)\geq 5/3$ by the fact that $\operatorname{rad}(a_1\cdot a_2\cdot a_3\cdot a_4)$ is a factor of $10\cdot(y+1)\cdot(x-1)\cdot(x^2+1)$ which is $O(x^3)$ due to $y+1$ and 10 being constant while $a_1=(x+1)^5$. □

Example 18. We have $Q_{U(\{1,2,3,4,6,7,12,14\},\emptyset,5)}\geq 7/4$.

This is witnessed by the quintuples of the form $((x+1)^7,-(x-1)^7,-14\cdot(x^2+1)^3,-28x^4,12)$, where $x=210^{k+2}$ and $k\in\mathbb{N}$. We do not provide further details of the proof, as the following example gives an even better bound.

Example 19. There is a finite set E with $Q_{U(E,\emptyset,5)}\geq 9/5$.

Proof. One chooses the following numbers:

1. $a_1=189(x+1)^9$;
2. $a_2=-189(x-1)^9$;
3. $a_3=-42(3x^2+7)^4$;
4. $a_4=16(63x^2+79)^2$;
5. $a_5=608$.

Here one chooses x itself to be 211^k-1 for some natural number k. Now one has that the greatest common divisor of a_1 and a_2 is 189, the one of $a_1\cdot a_2$ and a_3 is 21 times a factor of 10, the one of $a_1\cdot a_2$ and a_4 is a factor of 142 and the one of a_3 and a_4 is a factor of 136. The greatest common divisor of a_5 and any number is a factor of 608. Now choosing $E=\{r : r \text{ is a factor of one of the numbers } 136, 189, 142, 210, 608\}$ satisfies (i); note that $E\subseteq\{1,2,3,\ldots,608\}$.

One can verify by adding the polynomials that (ii) is satisfied. Condition (iii) holds for all sufficiently large x: when x is large, the subsum must also be 0 when viewed as a polynomial in x; for that reason, taking the degrees of the polynomials into account, either a_1, a_2 must both appear in the subsum or only a_5 appears which would then give the nonzero number a_5 or $-a_5$. If a_1 and a_2 both appear, then it must be of the form a_1+a_2 for eliminating the ninth power; as the result is a polynomial of degree 8, one has to subtract a_3 but then again the result is a

polynomial of degree 4, so the subsum needs to be $a_1 + a_2 + a_3 + a_4$ and has as result $-a_5$, so a_5 must also be added and the so (iii) is satisfied.

Condition (iv) is void.

One sees that $x+1$ is selected to be a power of a small number 211. So $\mathrm{rad}(a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5)$ is a factor of $189 \cdot 42 \cdot 16 \cdot 608 \cdot 211 \cdot (x-1) \cdot (3x^2+7) \cdot (63x^2+79)$ which is a polynomial in x of degree 5 while a_1 is a polynomial in x of degree 9; this gives the lower bound $9/5$ for large x. □

5 Gaussian Integers and the case $n = 4$

Gaussian integers (also called the complex integers) are integers augmented by the imaginary unit $\mathbf{i} = \sqrt{-1}$ and form the set $\mathbb{Z} + \mathbb{Z} \cdot \mathbf{i}$. Similarly, Eisenstein and others considered complex integers which have as units not the fourth roots of 1 but all sixth roots of 1. Wagon [21] gives some overview on this approach together with Mathematica algorithms to hand them. However, we decided to stick to the easier case of Gaussian integers.

The existence of complex roots allows to factorise numbers which are prime numbers in the ratioanl integers; here rational integers denote the elements of $\mathbb{Z}$, that is, they are those Gaussian integers which are at the same time rational numbers and do not have imaginary components [6]. For Gaussian integers, $2 = \mathbf{i} \cdot (1-\mathbf{i})^2$ and $5 = (2+\mathbf{i}) \cdot (2-\mathbf{i})$; in general, a rational integer $z \geq 2$ can be properly factorised if z is not a prime in the rational integers or $z = x^2 + y^2$ for two rational integers x, y where then $z = (x + y\mathbf{i}) \cdot (x - y\mathbf{i})$.

Let $C(E, F, n)$ denote the counterpart of $U(E, F, n)$ when allowing Gaussian integers in place of rational integers, here a Gaussian integer $x + y\mathbf{i}$ has the norm $x^2 + y^2$, the square root of this norm is called the absolute value. As norms are rational integers while the absolute value may be not, it is preferred to work with norms in number theory. The norm (or the absolute value) goes into the formula of the quality before taking the logarithms. Furthermore, primes in the Gaussian integers are defined such that they are neither units nor zero nor have other factors than units or products of themselves with units; two primes are associates if they can be obtained from each other by multiplying with units. Given an infinite set A of n-tuples of Gaussian integers with a one-one enumeration $\mathbf{a}_1, \mathbf{a}_2, \ldots$ where $\mathbf{a_k} = (a_{k,1}, \ldots, a_{k,n})$, the quality of the set A and its elements is defined as follows:

$$Q_A = \limsup_{k \to \infty} q(\mathbf{a}_k) \text{ where}$$

$$q(a_{k,1}, \ldots, a_{k,n}) = \frac{\log \max\{\mathrm{norm}(a_{k,1}), \ldots, \mathrm{norm}(a_{k,n})\}}{\mathrm{radnorm}(a_{k_1} \cdot \ldots \cdot a_{k,n})}.$$

Here $\mathrm{radnorm}(b)$ is the maximum of the norms of the products q of primefactors of b which are not associates of each other. Thus one looks at $Q_{C(E,F,n)}$ for the set $C(E, F, n)$ of all n-tuples $(a_1, a_2, \ldots, a_n)$ of Gaussian integers satisfying that no factor in F divides any component a_k and the common factors of a_i, a_j with $i \neq j$ are members of E and every sum with $\sum b_k a_k = 0$ and $b_k \in \{-1, 0, 1\}$ satisfies that either all b_k are 0 or all b_k are nonzero. In other words, $C(E, F, n)$ is the Gaussian integer analogue of the set $U(E, F, n)$ in the rational integers.

Darmon and Granville cite correspondence with Noam D. Elkies for various examples in their article; some of these examples imply that $Q_{C(\{1,2\},\emptyset,4)} > 1$.

Theorem 20 (Elkies [4]). *In the Gaussian integers,* $Q_{C(\{1\},\emptyset,4)} \geq 5/3$.

Proof. One of Elkies' examples [4, item (e) on page 542], shows the following polynomial identity of degree 5 for the complex rationals which, after multiplying with the denominators, can be brought into this form:

$$(x^2 + 2 \cdot x \cdot y - 2 \cdot y^2)^5 - (x^2 - 2 \cdot x \cdot y - 2 \cdot y^2)^5 + \mathbf{i} \cdot (-x^2 + 2\mathbf{i} \cdot x \cdot y - 2 \cdot y^2)^5 - \mathbf{i} \cdot (-x^2 - 2\mathbf{i} \cdot x \cdot y - 2 \cdot y^2)^5 = 0.$$

Denote the four additive terms with a^5, $-b^5$, $\mathbf{i} \cdot c^5$ and $-\mathbf{i} \cdot d^5$. One can see that $a - b$ and $c - d$ are, up to multiplications with units, products of x and $2y$. Furthermore, $a \cdot b - c \cdot d = (x^4 - 8x^2y^2 + 4y^4) - (x^4 + 8x^2y^2 + 4y^4) = -16x^2y^2$. Thus one can conclude that any common primefactor of two of these numbers is a factor of x or $2y$.

While Elkies' used this identity to solve equations where, when multiplied with some constant factors, two fifth powers and two tenth powers sum up to 0, we go another way and choose x and y such that $b = 1$, that is, that $x^2 - 2xy - 2y^2 = (x - y)^2 - 3y^2 = 1$. Here it is needed that x is odd. Now the greatest common divisor of x and $2y$ is 1, as otherwise the Pell equation would not have a solution, as when both x, y are multiples of p so is $(x - y)^2 - 3y^2$ and it could not be 1. Furthermore, no prime factor p of x or of $2y$ is a factor of a, b, c or d, as each of a, b, c, d is the sum of two multiples of p and one non-multiple of p. Thus no prime factors of x and $2y$ can be factors of a, b, c, d, but all common prime factors of two of a, b, c, d are also a prime factor of either x or $2y$. Thus a, b, c, d are pairwise coprime.

The so obtained choice allows to conclude that the largest of the four numbers has the norm

$$\max\{\text{norm}(a), \text{norm}(b), \text{norm}(c), \text{norm}(d)\}^5$$

while the norm of product of the three non-unit components is bounded from above by

$$\max\{\text{norm}(a), \text{norm}(b), \text{norm}(c), \text{norm}(d)\}^3$$

so that the quality is at least $5/3$.

This result can be, using the Pell equation technique, generalised to the following one.

Theorem 21. *If* $n \geq 4$ *and* F *is a finite set of Gaussian integers which contains neither units nor units multiplied with* $1 + \mathbf{i}$ *then* $Q_{C(\{1\},F,n)} \geq 5/3$.

Proof. Let s be the product of all norms of members of F times 2310; note that the norm of a complex number is the square of its real part plus the square of its imaginary part, for example, the norm of $7 + 9\mathbf{i}$ is $7^2 + 9^2 = 130$. If n is odd then let $m = 5$ else let $m = 4$. If $n > 5$ then one chooses $n - m - 2$ odd prime numbers (in the rational integers) $a_n, a_{n-1}, \ldots, a_{m+2}$ such that each of them is larger than s and thus coprime to all members of F and each a_{k-1} is at least five

times as large as a_k and each prime $a_n, a_{n-1}, \ldots, a_{m+2}$ has modulo 4 the value 3, so that these prime numbers are also prime numbers in the Gaussian integers. Now let t be the product of s and the absolute values of $a_{m+2}, a_{m+3}, \ldots, a_n$; furthermore, choose using Proposition 12 a_m and a_{m+1} to be rational integers such that $1 + \sum_{k=m,\ldots,n} a_k = 0$ and no rational prime number below $10 \cdot t$ divides either a_m or a_{m+1}. Let $u = t \cdot a_m \cdot a_{m+1}$.

If $n = m$, that is, $n \in \{4, 5\}$, one skips the above and just selects u to be t as calculated above and a_m will be chosen as below.

Now one let (v, w) be a sufficiently large solution of the Pell Equation $v^2 - w^2 \cdot 3u^2 = 1$; as $3u^2$ is not a perfect square, it follows from a Theorem of Lagrange that there are infinitely many such pairs (v, w). Now let $y = u \cdot w$ and $x = v + u \cdot w$ and let in the case that n is even

$$\begin{aligned}
a_1 &= (x^2 + 2xy - 2y^2)^5, \\
-1 &= -(x^2 - 2 \cdot x \cdot y - 2 \cdot y^2)^5, \\
a_2 &= \mathbf{i} \cdot (-x^2 + 2\mathbf{i} \cdot x \cdot y - 2 \cdot y^2)^5, \\
a_3 &= -\mathbf{i} \cdot (-x^2 - 2\mathbf{i} \cdot x \cdot y - 2 \cdot y^2)^5, \\
a_4 &= -1 \text{ in the case that } n = 4,
\end{aligned}$$

and in the case of n being odd (including the so far ignored case $n = 5$),

$$\begin{aligned}
a_1 &= \mathbf{i} \cdot (x^2 + 2xy - 2y^2)^5, \\
-\mathbf{i} &= -\mathbf{i} \cdot (x^2 - 2 \cdot x \cdot y - 2 \cdot y^2)^5, \\
a_2 &= \mathbf{i}^2 \cdot (-x^2 + 2\mathbf{i} \cdot x \cdot y - 2 \cdot y^2)^5, \\
a_3 &= -\mathbf{i}^2 \cdot (-x^2 - 2\mathbf{i} \cdot x \cdot y - 2 \cdot y^2)^5, \\
a_4 &= 1 - \mathbf{i}, \\
a_5 &= -1 \text{ in the case that } n = 5,
\end{aligned}$$

that is, one multiplies the numbers of the case of n being odd with $\mathbf{i}$ and adds a_4 as one even Gaussian integer to allow all others to be odd; note that here a Gaussian integer is even iff the sum of the two coordinates is even iff the Gaussian integer is not coprime to 2. Furthermore, for $n = m$, one let a_m be -1 what is otherwise the sum of $\sum_{k=m,\ldots,n} a_m$. Note that the second equation is in both cases satisfied by the choice of x, y and that the other three numbers are chosen in the same way as in Theorem 20. Note that all members of F and $2, a_m, a_{m+1}, \ldots, a_n$ are factors of u and thus of y and therefore a_1, a_2, a_3 are coprime to these numbers, as proven in Theorem 20. Furthermore, if n is odd then a_4 is the only even number and it is a prime number of the Gaussian integers dividing 2. Here prime numbers p in the Gaussian integers are considered to be identical with $-p, \mathbf{i} \cdot p, -\mathbf{i} \cdot p$.

It remains to show the subsum property. For this let p be a rational integer prime factor of either a_m or a_{m+1}. Now consider the case that p divides a_m, the case of a divider of a_{m+1} is symmetric. So a_m is 0 modulo p. Furthermore, note that y is 0 modulo p and therefore $x = 1$ modulo p. The primes $a_{m+2}, a_{m+3}, \ldots, a_n$ are all equal to themselves and smaller than $p/2 - 5$ when taken as remainder of the division by p. Thus one has the following situation modulo p:

If n is even
then $m = 4$ and $a_1 + a_2 + a_3 = 1$ and $1 + \sum_{k>m} a_k = 0$
else $m = 5$ and $a_1 + a_2 + a_3 + a_4 = 1$ and $1 + \sum_{k>m} a_k = 0$.

In summary $\sum_{k<m} a_k = 1$. Furthermore, the numbers $a_{m+2}, \ldots, a_n$ are all at least 11 and form an ascending chain of numbers smaller than $p/2 - 5$ with each member being five times larger than the previous one and their sum is, modulo p, equal to $-a_{m+1}$. Only the numbers $a_1, a_2, \ldots, a_{m-1}$ have an imaginary component and the same is true modulo p, where one considers them as a real number from $\{0, 1, \ldots, p-1\}$ added with an imaginary number from $\mathbf{i} \cdot \{0, 1, \ldots, p-1\}$ and for the ease of notation, one identifies $-k$ with $p - k$. As a_{m+1} is the sum of the others and the first $m-1$ of them have norms bounded by 2 and the others form sum of each term in the sum being more than five times the previous one and thus more than the sum of the absolute values of the previous ones, the only possible nontrivial zero sums of these numbers involve $a_1, a_2, \ldots, a_{m-1}$ and a_m. However, if p would be a factor of a_{m+1}, one would conclude that the only nontrivial zero sums of this numbers involve $a_1, a_2, \ldots, a_{m-1}$ and a_{m+1}. The combination of this gives that the only nontrivial sum, if any, would be $\sum_{k<m} a_k \cdot b_k$ with $b_k \in \{-1, 0, 1\}$. These have to be 0 also modulo p and therefore one has to look at the following possible cases.

If n is even then this would only be the case $a_2 - a_3 = 0$, however, it follows from the proof of Theorem 20 that for the full numbers without remainder that this subsum is not 0. If n is odd then there are the cases $a_2 - a_3 = 0$ (already excluded), $a_1 + a_4 - a_2 = 0$ and $a_1 + a_4 + a_3 = 0$. To exclude the other two, one takes a prime number q dividing x and gets, modulo q, that $-2y^2 = 1$. It follows that the values of $a_1 + a_4 - a_2$ and $a_1 + a_4 + a_3$ are, modulo q, both 2, not 0. Thus no nontrivial subsum gives 0.

Furthermore, in the case $n = 5$, there are more possible equalities modulo p; here p is a prime factor of v and q is a prime factor of $u \cdot w$ and thus modulo p, $2y = 0$ and $x^2 = 1$; modulo q, $x = 0$ and $-2y^2 = 1$. Modulo p, the nontrivial subsums are as follows: $a_2 + a_3 = 0$, $a_2 + a_5 = 0$, $-a_3 + a_5 = 0$, $a_1 + a_4 + a_3 = 0$, $a_1 + a_4 - a_2 = 0$, $a_1 + a_4 + a_5 = 0$. Modulo q, the nontrivial subsums are as follows: $a_2 + a_3 = 0$, $-a_2 + a_5 = 0$, $a_3 + a_5 = 0$, $a_1 + a_4 - a_3 = 0$, $a_1 + a_4 + a_2 = 0$, $a_1 + a_4 + a_5 = 0$. Now one considers only those nontrivial subsums which occur both modulo p and modulo q and these are $a_2 + a_3 = 0$ and $a_1 + a_4 + a_5 = 0$. The first one was excluded in Theorem 20 and the second one says implies that $(x^2 + 2xy - y^2)^5 - 1 = 0$. As $x^2 - 2xy - y^2 = 1$, this equation equals to $(1 + 4xy)^5 - 1 = 0$ and that is not satisfied, as x and y are both integers which are not zero. So there is no nontrivial subsum for $n = 5$. In the case that $n = 4$, it is already shown in Theorem 20 that there are no nontrivial subsums.

Note, however, that the numbers $a_1, \ldots, a_n$ are chosen such that if all b_k are 1 then they sum up to 0. Furthermore, the values $a_4, \ldots, a_n$ are all constant in the construction while a_1, a_2, a_3 depend on v, w and can be arbitrary large. Let

$$d = \max\{|x^2 + 2xy - 2y^2|, |-x^2 + 2\mathbf{i} \cdot xy - 2y^2|, |-x^2 - 2\mathbf{i} \cdot xy - 2y^2|\}$$

and one has the the quality is at least the quotient of $\log(d^5)$ and $\log(d^3 \cdot c)$ where the constant part c is the product $a_4 \cdot a_5 \cdot \ldots \cdot a_n$ which is independent of d and d can be made as large as possible. Thus one has that, in the Gaussian integers, $Q_{C(\{1\},F,n)} \geq 5/3$ for all $n \geq 4$.

Example 22. This example shows that in the Gaussian integers, $Q_{C(\{1\},F,4)} \geq 5/3$ for the set F of all prime factors of $2, 3, 5, 7$ and $Q_{U(\{1\},\emptyset,6)} \geq 5/3$.

Although this follows already from the previous theorem, a more direct construction is given in order to illustrate the previous result; however, this construction does not follow the proof exactly but has a simpler, more explicit proof idea.

Note that $z_0 = 3650401$ and $y_0 = 2107560$ satisfy $z_0^2 - 3y_0^2 = 1$. Furthermore, $y_0 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 193$. So $x_0 = z_0 + y_0$ and y_0 provide a, b, c, d as required in Theorem 20 based on Elkies' identity and all of a, b, c, d do not have any common prime factors with $2, 3, 5, 7$ in the Gaussian integers. The same is true for all x_n, y_n, z_n derived from x_0, y_0, z_0 by

$$(x_{n+1}, y_{n+1}, z_{n+1}) = (2 \cdot y_n \cdot z_n + 2 \cdot z_n^2 - 1, 2 \cdot y_n \cdot z_n, 2 \cdot z_n^2 - 1)$$

as all y_n are multiples of y_0. Now let a_n, b_n, c_n, d_n be derived from x_n, y_n as in Theorem 20 and recall that

$$a_n^5 - b_n^5 + \mathbf{i} \cdot c_n^5 - \mathbf{i} \cdot d_n^5 = 0.$$

As $b_n = 1$ by the choice of x_n, y_n, z_n and as none of a_n, b_n, c_n, d_n has a prime factor in common with $3, 5, 7$, one gets the equality

$$a_n^5 + \mathbf{i} \cdot c_n^5 - \mathbf{i} \cdot d_n^5 + 7 - 5 - 3 = 0$$

and all its members are coprime. Furthermore, only the second and third term contain an imaginary component and thus every subsum must either omit both terms or have them in the same way added (or negated) as above. When omitted, as one needs an even number of terms to make the sum of odd numbers to 0, a_n^5 cannot be part of it, as its absolute value is much above $3 + 5 + 7$. Furthermore, any sum of two would not give 0, as the sum above does not contain any v, w with $v = w$ or $v = -w$. So the part $a_n^5 + \mathbf{i} \cdot c_n^5 - \mathbf{i} \cdot d_n^5$ must be part of any subsum, as otherwise no combination of $3, 5, 7$ can make it 0. However, this subsum and its negation only take the values -1 and 1 and no single of $3, 5, 7$ can make these 0. Hence there are no proper subsums which make the signed sum of less than the six terms to be 0. This completes the proof of the claims in this example.

6 Hamiltonian Integers and the case $n = 3$

Hamilton discovered that one can get a skew field extension over the reals by introducing three square roots $\mathbf{i}, \mathbf{j}$ and $\mathbf{k}$ of -1 which do not commute. Hamiltonian integers are then the restriction of this structure to numbers of the form $q + r\mathbf{i} + s\mathbf{j} + t\mathbf{k}$ with $q, r, s, t \in \mathbb{Z}$. These numbers form a ring with 1 and the multiplication of integers with these ring elements commutes, but for the imaginary units the rules $\mathbf{i} \cdot \mathbf{j} = \mathbf{k}, \mathbf{i} \cdot \mathbf{k} = -\mathbf{j}, \mathbf{j} \cdot \mathbf{k} = \mathbf{i}$ and $v \cdot w = -v \cdot w$ for distinct $v, w \in \{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Hardy and Wright [6] give an overview over the Hamiltonian integers, but they also consider the additional half integers introduced by Hurwitz [8]; Remark 29 below gives more details of this concept, though we for our work stick to the easier way to define Hamiltonian integers.

Due to noncommutativity, there are certain aspects where the Hamiltonian integers differ from the rational integers or the Gaussian integers. For example,

$$13 = -1 \cdot (2\mathbf{i} + 3\mathbf{j})^2 = -1 \cdot (1 + 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k}) \cdot (1 - 2\mathbf{i} - 2\mathbf{j} - 2\mathbf{k}).$$

The norm of a Hamiltonian integer $q + r\mathbf{i} + s\mathbf{j} + t\mathbf{k}$ is the number $q^2 + r^2 + s^2 + t^2$ – note that many authors take the square-root of this sum, but this leads here to non-integer values what is undesirable. The norm of a product is the product of the norms of the factors. A factorisation of a Hamiltonian integer x is any product of Hamlitonian integers whose value is x. A facorisation of a tuple (x, y, z) is the product of the factorisations of x, y, z, but not the factorisation of $x \cdot y \cdot z$, as that can have optimiations which the product of factorisations does not have. The radical of a number or tuple is a factorisation from which one has deleted any entry which occured in the factorisation already before in the same exact form. So the radical of $-1 \cdot (2\mathbf{i}+3\mathbf{j})^2$ is $-1 \cdot (2\mathbf{i}+3\mathbf{j})$ and the radical of $-1 \cdot (1 + 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k}) \cdot (1 - 2\mathbf{i} - 2\mathbf{j} - 2\mathbf{k})$ is that factorisation itself. Thus the two factorisations of 13 above have two different radicals. The radnorm of a number or a tuple is the smallest norm taken by any factorisation of this number or tuple. Due to the first factorisation, the radnorm of 13 is 13; the second factorisation would give the norm 169 and is thus suboptimal. The next example shows that there is a reason for defining the radnorm of tuples differently from the radnorm of the product of their members.

Example 23. $\text{radnorm}(2, 7) > \text{radnorm}(14)$.

Proof. Note that $14 = -1 \cdot (3\mathbf{i} + 2\mathbf{j} + \mathbf{k})^2$ has the radnorm $1 \cdot (3^2 + 2^2 + 1^2) = 14$. As 14 is the product of two different prime numbers and each prime number divides the radnorm of a natural number, this value is optimal. Now assume that $7 = u \cdot x \cdot v \cdot x \cdot w$ where u, v, w are units. The norm of x has to be 7 and now the task is to show that this factorisation does not exist; as products of units are units, one can without loss of generality assume that in a factorisation, two neighbouring units are merged into one. Now one multiplies 7 with $v \cdot u^{-1}$ from the front and with $u \cdot v^{-1} \cdot -1$ from the back. Note that the units commute with 7 and there is no sign change. Furthermore, $v \cdot u^{-1} \cdot u = v$. For the back side, let $w' = w \cdot u \cdot v^{-1}$. Furthermore, let $y = u \cdot x$. Note that y and $u \cdot x$ have the same norm, as the norm is multiplicative and u is a unit. Now the equation is $7 = y \cdot y \cdot w'$. The norm of y must be 7. As 7 is not the sum of three squares, the value of y must be equal to $q + r\mathbf{i} + s\mathbf{j} + t\mathbf{k}$ with three of these coefficients have the absolute value 1 and one has the absolute value 2. Now the new value in the first position is $q^2 - r^2 - s^2 - t^2$ which differs from -7 and $+7$. It also differs from 0 as it is the sum of one even and three odd integers, independently on how the sign of these integers is taken. Thus the full number must have also at least one nonzero imaginary component. Multiplying it with w' preserves the number of nonzero components in the number and the number is not 7. Hence there is no factorisation of 7 with two equal factors of norm 7 and so $\text{radnorm}(7) = 49$. Furthermore, $\text{radnorm}(2) = 2$, as $2 = -1 \cdot (\mathbf{i} + \mathbf{j})^2$. So $\text{radnorm}(2, 7) = 98$. □

Note that exactly the natural numbers of the form $4^a \cdot (8b + 7)$ cannot be written as the sum of three squares and that thus prime numbers of this form cannot be written as $u \cdot y^2$ for any unit u

by the above proof. Indeed, one can show that these are the only prime numbers which cannot be factorised this way. All others prime numbers p are of the form $r^2+s^2+t^2$ with $r,s,t\in\mathbb{N}$ and thsu $p=-1\cdot(r\mathbf{i}+s\mathbf{j}+t\mathbf{k})^2$ which gives that $\mathrm{radnorm}(p)=p$. Furthermore, note that for composite numbers of the above form, one can sometimes prove that their radnorm is smaller than their norm. An example is that $\mathrm{radnorm}(27559)=\mathrm{radnorm}(7\cdot 3937)\leq \mathrm{norm}(7)\cdot\mathrm{norm}(60\mathbf{i}+16\mathbf{j}+9\mathbf{k})=49\cdot 3937=192913$ while $\mathrm{norm}(27559)=759498481$. Note that $27559=3444\cdot 8+7=7\cdot 31\cdot 127$, so it is the product of three prime numbers of the form $8b+7$. The preceding discussions justify the following definition.

Let $H(E,F,n)$ be as in the definition of $U(E,F,n)$ with the only difference that one uses Hamiltonian integers instead of rational integers; the restrictions on F are modified in the sense that F does not contain units and that no member of F occurs as factor in any factorisation of the n-tuple. Furthermore, let $H'(F,n)$ be the adjustment of the the set $B(n)$ from the n-conjecture to Hamiltonian integers such that no member of any factorisation of an n-tuple in $H'(F,n)$ contains any factor from F and that no nonzero nonunit occurs as factor in some factorisation of each member of the tuple. The numbers $Q_{H(E,F,n)}$ and $Q_{H'(F,n)}$ are defined analogously. The main interest in this section is with the notions of $Q_{H(\{1\},F,3)}$ and $Q_{H'(F,3)}$. Here for any infinite set A of Hamiltonian tuples, of all n-tuples in A and any tuple $\boldsymbol{a}=(a_1,a_2,\ldots,a_n)$, one defines the following notions:

$$\begin{aligned}\mathrm{maxnorm}(\boldsymbol{a})&=\max\{\mathrm{norm}(a_1),\mathrm{norm}(a_2),\ldots,\mathrm{norm}(a_n)\};\\ q(\boldsymbol{a})&=\frac{\log(\mathrm{maxnorm}(\boldsymbol{a}))}{\log(\mathrm{radnorm}(\boldsymbol{a}))};\\ Q_{\{\boldsymbol{a}_1,\boldsymbol{a}_2,\ldots\}}&=\limsup_{k\to\infty} q(\boldsymbol{a}_k).\end{aligned}$$

Here $\boldsymbol{a}_1,\boldsymbol{a}_2,\ldots$ is a one-one enumeration of some infinite set A of n-tuples in the Hamiltonian integers. Natural choices for A are $A=H(E,F,n)$ or $A=H'(F,n)$ as defined above. Furthermore, $q(a_1,a_2,\ldots,a_n)$ is called the quality of the tuple $(a_1,a_2,\ldots,a_n)$.

Note that a square gives a linear factor in the logarithm which cancels out, thus it does not make a difference if one defines the norm as in this paper or as one takes always the square-root of the norm as done by many other authors. The next result shows that due to root-taking, even for integer tuples, the quality of the tuple can be at least 2.

Example 24. For given h, let $(a_h,b_h,c_h)=(2^h,1,-2^h-1)$ and note that for even $h=2\ell$, $-2^h-1=(2^\ell\mathbf{i}+\mathbf{k})^2$ and for odd $h=2\ell+1$, $-2^h-1=(2^\ell\mathbf{i}+2^\ell\mathbf{j}+\mathbf{k})^2$. Thus

$$q(a_h,b_h,c_h)\geq\frac{\log(2^{2h})}{\log(2^{h+2})}=2\cdot\frac{h}{h+2}$$

and $Q_{H(\{1\},\emptyset,3)}\geq 2$. So the abc-conjecture needs, for Hamiltonian integers, even if the numbers itself are integers, at least constant 2.

Furthermore, note that if F is a set of odd integers, that is of integers with odd norm, then the product of all numbers in F and of their conjugates — the conjugate of $q+r\mathbf{i}+s\mathbf{j}+t\mathbf{k}$ is

$q - r\mathbf{i} - s\mathbf{j} - t\mathbf{k}$ — gives then an odd number ℓ which is a multiple of all norms of the numbers in F and also a multiple of all numbers in F. Now choosing $h = \ell!$ in the above makes sure that every rational prime number p dividing ℓ satisfies that 2^h modulo p is 1 and thus $2^h + 1$ modulo p is 2, so p is no factor of this number. Furthermore, all odd numbers are coprime with powers of 2. Thus for any finite set F of odd Hamiltonian integers there are infinitely many h such that $2^h, 2^h + 1, 1$ are all coprime to all members in F and therefore, for such F, $Q_{H(\{1\},F,3)} \geq 2$ as well.

The same lower bound can be obtained by studying Pell equations.

Example 25. Let c be a natural number which is not a perfect square. Then $v^2 - c \cdot w^2 = 1$ has infinitely many solutions in the rational integers. Furthermore, $x^4 - c \cdot y^4 = 1$ and $x^4 - c \cdot (\mathbf{i}+\mathbf{j})^4 \cdot y^4 = 1$ both have infinitely many solutions in the Hamiltonian integers.

Proof. The solution of each Pell equation in the rational integers is well-known; Lenstra [9] provides an overview and explain's Lagrange's proof for this. Now let (v, w) be a solution of the equation such that w is a multiple of 8. Note that whenever (v, w) is a solution, so is $(v^2 + c \cdot w^2, 2vw)$; repeating this process 3 times gets w to be a multiple of 8 as assumed. Now the number $v^2 + c \cdot w^2$ is equal to 1 modulo 8, as $v^2 + c \cdot w^2$ has to be odd. Note that squares modulo 8 are either 0 or 1 or 4. Now Legendre's Three-Square Theorem – see, for instance, Shiu [16] – says that numbers which are not of the form $4^2 \cdot (8b+7)$ are the sum of three squares. So $v^2 + cw^2$ is the sum of three squares $r^2 + s^2 + t^2$ and equal to $-x^2$ for $x = r\mathbf{i} + s\mathbf{j} + t\mathbf{k}$. At least one of vw and $2vw$ is not of the form $4^a \cdot (8b + 7)$, as one of them has an odd number of prime factors 2. Furthermore, note that when v is 1 modulo 8, then the mapping $(v, w) \mapsto (v^2 + c \cdot w^2, 2vw)$ maps solutions of the Pell equation to new solutions and changes the number of occurrences of the prime factor 2 in the second number from even to odd or odd to even, thus there are infinitely many solutions (v, w) of the Pell equation $v^2 - c \cdot w^2 = 1$ in the rational integers where vw is the sum of three squares and furthermore infinitely many solutions (v, w) where $2vw$ is the sum of three squares.

First consider numbers v, w where $2vw$ is not of the form $4^a \cdot (8b+7)$. Then $2vw$ is of the sum of three squares and thus equal to $-y^2$ for a Hamiltonian integer y. It follows that $x^4 - cy^4 = 1$.

Second consider numbers v, w where vw is not of the form $4^a \cdot (8b + 7)$, then vw is equal to $-y^2$ for some Hamiltonian integer y and $c(2vw)^2 = c \cdot 4 \cdot (vw)^2 = c \cdot (\mathbf{i} + \mathbf{j})^4 \cdot y^4$ for this Hamiltonian integer y. Now one gets a solution for $x^4 - c \cdot (\mathbf{i} + \mathbf{j})^4 \cdot y^4$. □

The above examples showed that for *abc*-triples given by rational integer, the facorisation in the Hamiltonian integers gives at least the lower bound 2 instead of 1. The next proposition says if one can construct systematically *abc*-triples of rational integers which have with respect to factorising in Hamilitonian integers all a quality above $2 + 2\varepsilon$ then one has indeed proven that in the rational integers the *abc*-conjecture has at least lower bound $1 + \varepsilon$.

Proposition 26. *Let $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ be a tuple of rational nonzero integers having the sum 0 and let $q_{\mathbb{H}}(\boldsymbol{a})$ be the quality of $\boldsymbol{a}$ with respect to factorisation in the Hamiltonian integers and*

$q_{\mathbb{Z}}(\boldsymbol{a})$ *be the quality of* $\boldsymbol{a}$ *with respect to factorisation in the rational integers. Now* $q_{\mathbb{Z}}(\boldsymbol{a}) \leq q_{\mathbb{H}}(\boldsymbol{a}) \leq 2q_{\mathbb{Z}}(\boldsymbol{a})$.

For all applicable E, F, n,

$$Q_{U(E,F,n)} \leq Q_{H(E,F,n)\cap\mathbb{Z}^n} \leq 2 \cdot Q_{U(E,F,n)} \text{ and } Q_{A(n)} \leq Q_{H'(\emptyset,n)\cap\mathbb{Z}^n} \leq 2 \cdot Q_{A(n)},$$

where the Q *on the middle of each sequence of inequalities refers to factorisation in the Hamiltonian integers and the other two numbers to factorisation in the rational integers.*

Proof. Note that in factorisations the part of the norm contributed by units is 1 and thus one can multiply out two neighbouring units belonging to the same component of the tuple without changing the norm of the factorisation. As the product of the norms is the norm of the product and as every norm of a nonzero Hamiltonian integer is a nonzero natural number, there are only finitely many factorisations which have to be taken into account. One of the factorisations of the tuple, call it $x_1 \cdot x_2 \cdot \ldots \cdot x_m$ witnesses the value of the radnorm of the tuple. Each prime p in the natural nubmers is a factor of $\text{norm}(a_1) \cdot \text{norm}(a_2) \cdot \ldots \cdot \text{norm}(a_n)$ iff it is a factor of the integer $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ iff it is a factor of $\text{norm}(x_1) \cdot \text{norm}(x_2) \cdot \ldots \cdot \text{norm}(x_m)$.

Thus $\text{radnorm}(a_1, a_2, \ldots, a_n)$ consists of the product of $\text{norm}(x_k)$ of those x_k which occur at position k for the first time in the factorisation; thus $\text{radnorm}(\mathbf{a})$ is a multiple of the radical of $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ as integers. Furthermore, $\text{radnorm}(\boldsymbol{a})$ is bounded from above by the square of the radical of $a_1 \cdot a_2 \cdot \ldots \cdot a_n$, as one could just take the rational integer factorisation of the tuple and use that for integer primes p, $\text{norm}(p) = p^2$. So while in the $q_{\mathbb{H}}(\mathbf{a})$ the numerator is just twice the value of $q_{\mathbb{Z}}(\mathbf{a})$, the denominator is between that of $q_{\mathbb{Z}}(\mathbf{a})$ and twice that of $q_{\mathbb{Z}}(\mathbf{a})$. This then directly gives the inequality $q_{\mathbb{Z}}(\boldsymbol{a}) \leq q_{\mathbb{H}}(\boldsymbol{a}) \leq 2q_{\mathbb{Z}}(\boldsymbol{a})$.

The inequalities of the second equation follow directly from those for the qualities of the tuples. □

It is an open question whether the third statement also holds in the case that one does not require the tuples to be integer-triples.

Hardy and Wright [6, Theorem 374] show that every two Hamiltonian integers have a greatest common right hand divisor. Note that this one is then also a right-hand divisor of the sum. For this, however, it is needed that in both cases no factor is on the right side of the divisor, not even two different units. However, it is not true that if a Hamiltonian integer appears in the factorisations of two Hamiltonian integers that it then also appears in the factorisation of the sum. This is if two numbers are multiples of a number then so is there sum. This is due to the noncommutativity of the multiplication. The next example uses this to prove that $Q_{H'(\emptyset,3)} \geq 4$. By definition the example cannot be used for showing $Q_{H(\{1\},\emptyset,3)} \geq 4$; indeed, we were unable to find any systematic construction of examples showing a lower bound beyond 2.

Theorem 27. *For all* $n \geq 3$, $Q_{H'(\emptyset,n)} \geq 4 \cdot (2n - 5)$.

Proof. Let (a, b) be a solution to the Pell equation $a^2 - 2b^2 = 1$, recall that there are infinitely many such solutions. Now let $y = a + b\mathbf{i} + b\mathbf{j}$. Now y^2 is $1 + 2ab\mathbf{i} + 2ab\mathbf{j}$. Now one conisders $-\mathbf{i} \cdot y^2 \cdot \mathbf{i}$ which is $1 + 2ab\mathbf{i} - 2ab\mathbf{j}$. The product $x = y^2 \cdot -\mathbf{i} \cdot y^2 \cdot \mathbf{i}$ is $1 + 4ab\mathbf{i} - 8a^2b^2\mathbf{k}$. Note that

this number is odd and that $\bar{x} = -\mathbf{j} \cdot x \cdot \mathbf{j}$. The sum $x + \bar{x} = 2$. As one can choose y to have an arbitrarily large norm, the norms of $x, \bar{x}$ satisfy $\text{norm}(x) = \text{norm}(y)^4$ and the quality of the tuple $(x, \bar{x}, -2)$ is $4\log(\text{norm}(y))/(\log(\text{norm}(y)) + \log(2))$ and as $\log(2)$ is constant in this term, the limit superior of these qualities is 4.

For the bounds of the n-conjecture in general, one considers formulas computing $x^{2n-5} + \bar{x}^{2n-5}$ which can be obtained by the following recursive equations, the first one is the general recursion formula and then follow two starting equations; the remaining equations are computed with a computer program using the recursion formula; the recursion formula is based on the fact that $x\bar{x} = \bar{x}x = \text{norm}(x)$ as well as $x^{n+2} = 2 \cdot x^{n+1} - \bar{x} \cdot x^{n+1}$ and $\bar{x}^{n+2} = 2 \cdot \bar{x}^{n+1} - x \cdot \bar{x}^{n+1}$:

$$\begin{aligned}
x^{n+2} + \bar{x}^{n+2} &= 2 \cdot (x^{n+1} + \bar{x}^{n+1}) - \text{norm}(x) \cdot (x^n + \bar{x}^n);\\
x^0 + \bar{x}^0 &= 2;\\
x + \bar{x} &= 2;\\
x^2 + \bar{x}^2 &= 4 - 2 \cdot \text{norm}(x);\\
x^3 + \bar{x}^3 &= 8 - 6 \cdot \text{norm}(x);\\
x^4 + \bar{x}^4 &= 16 - 16 \cdot \text{norm}(x) + 2 \cdot \text{norm}(x)^2;\\
x^5 + \bar{x}^5 &= 32 - 40 \cdot \text{norm}(x) + 10 \cdot \text{norm}(x)^2;\\
x^6 + \bar{x}^6 &= 64 - 96 \cdot \text{norm}(x) + 36 \cdot \text{norm}(x)^2 - 2 \cdot \text{norm}(x)^3;\\
x^7 + \bar{x}^7 &= 128 - 224 \cdot \text{norm}(x) + 112 \cdot \text{norm}(x)^2 - 14 \cdot \text{norm}(x)^3.
\end{aligned}$$

So $x^{2m} + \bar{x}^{2m}$ are $x^{2m+1} + \bar{x}^{2m+1}$ are both polynomials of degree m in $\text{norm}(x)$ with coefficients independent of x (as long as chosen such that $x + \bar{x} = 2$) and one can see by the induction formula that this property is preserved. Furthermore, the coefficients of even powers of $\text{norm}(x)$ are nonnegative and those of odd powers of $\text{norm}(x)$ are nonpositive. One can see that the updating in the recursion formula makes the absolute values of these coefficients larger, as the minused-out term is multiplied with $\text{norm}(x)$, and that for each even degree $2m$, the m-th power gets the coefficient $(-1)^m \cdot 2$. The latter can be seen from the fact that when forming the polynomial for $x^{2m+2} + \bar{x}^{2m+2}$, one multiplies the polynomial for $2m$ with $\text{norm}(x)$ and adds to it 2 times the polynomial for $x^{2m+1} + \bar{x}^{2m+1}$. Similarly one sees that the calculation of the polynomial $x^{2m+3} + \bar{x}^{2m+3}$ can make coefficients only have large absolute values, not smaller ones. Thus the coefficients for $\text{norm}(x)^0, \ldots, \text{norm}(x)^m$ are in the polynomials for $x^{2m} + \bar{x}^{2m}$ and $x^{2m+1} + \bar{x}^{2m+1}$ nonzero and alternating in sign.

Furthermore, as y is odd, so is also x. The constant term in each equation is 2^m, as one can split $(x + \bar{x})^m = 2^m$ into two pure terms x^m and $\bar{x}^m$ and mixed terms which all allow to bracket out $\text{norm}(x) = x\bar{x}$. 2^m is coprime to any odd number in the Hamiltonian integers.

For the subsum property, note that if one subtracts out one subsum giving 0, the other remaining subsum is also 0 and both have $\{0, 1\}$-valued coefficients for the term. As $x^m, \bar{x}^m$ are the only numbers with imaginary components, these numbers have both to go into one of the two subsums, so one considers the other one. For the other subsum, one can assume that x is so large that $\text{norm}(x)$ is at least 3 times any absolute value of a coefficient in the equation. Thus the subsum is a telescope sum where the lower-order terms of $\text{norm}(x)^k$ cannot compensate the

impact of the highest nonzero term. Therefore this subsum must have all coefficients 0 and so the subsum property of the n-conjecture is satisfied whenever the (a, b) in $y = a + b\mathbf{i} + b\mathbf{j}$ is chosen to be sufficiently large solutions of the Pell equation $a^2 - 2b^2 = 1$.

So one chooses for the n-conjecture $m = 2n - 5$ and obtains an equation with the two terms $x^m, \bar{x}^m$ plus $^{m+1}/_2$ terms of fixed coefficients $c_{n,h}$ multiplied with $\text{norm}(x)^h$ for $h = 0, 1, \ldots, m$. This gives n terms in total and the tuple considered is of the form

$$\mathbf{a} = (x^{2n-5}, \bar{x}^{2n-5}, c_{n,0}, c_{n,1} \cdot \text{norm}(x), c_{n,2} \cdot \text{norm}(x)^2, \ldots, c_{n,n-3} \cdot \text{norm}(x)^{n-3})$$

Now $\text{maxnorm}(\mathbf{a}) = \text{norm}(x^{2n-5}) = \text{norm}(y)^{4 \cdot (2n-5)}$; note that $\text{norm}(x) = \text{norm}(y)^4$; here one assumes that y is chosen such that $\text{norm}(x) > \text{norm}(c_{n,h})$ for all h; note that $\text{norm}(\text{norm}(x)) = \text{norm}(x)^2$ at the evaluation of the norms of terms $\text{norm}(x)^h$. Furthermore, $\text{radnorm}(\mathbf{a})$ is a factor of $\text{norm}(y \cdot \prod_{h=0}^{n-3} c_{n,h})$ and therefore the quality is at least the limit superior of the expressions $4(2n-5)\log(\text{norm}(y))/(\log(\text{norm}(y)) + \log(\text{norm}(\tilde{c})))$, where $\tilde{c}$ is the product of all coefficients; as y can be chosen to have arbitrarily large norm without changing the coefficients, the quality of the n-conjecture in the Hamiltonian integers is at least $4 \cdot (2n - 5)$. □

This result indicates that there might be some difference between the normal and the strong version of the *abc*-conjecture for Hamiltonian integers, as the lower bounds obtained differ by a factor 2. Note that these two versions coincide for the rational and Gaussian integers.

One can also show that in various preceeding results for $Q_{U(E,F,n)}$, the construction of the big factors (which depend on x) are natural numbers which are not of the form $4^a \cdot (8b + 7)$ and therefore these can be written as -1 times a square of a Hamiltonian integer. Thus one obtains the following corollary.

Corollary 28. **(a)** *Let E and F be arbitrary and let $n \geq 6$. Then $Q_{H(E,F,n)} \geq {}^5/_2$.*
(b) *For odd $n \geq 5$, $Q_{H(\{1\},\emptyset,n)} \geq {}^{10}/_3$.*

Proof. First one has to note that if the norm of two Hamiltonian integers is coprime then they are also coprime as Hamiltonian integers. This comes due to the fact that a common nonunit factor has a norm of at least 2 which divides the norm of each multiple. Thus if the numbers $a_1, a_2, \ldots, a_n$ are pairwise coprime as rational integers, then they are also pairwise coprime as Hamiltonian integers.

(a): For the result from Theorem 13, note that the entity y there is a multiple of 8 and that x is of the form $(y + 1)^{h!}$, so x is of the form $8b + 1$ and not of the form $8b + 7$. The same is true for $x + y$, $x - y$ and $x^2 + 10y^3$. It follows that all the big factors which depend on x are the product of -1 and a square in the Hamiltonian integers. Thus the n-tuples given in Theorem 13 (depending on the parameter h) actually witnesses that in the Hamiltonian integers $Q_{H(\{1\},F,n)} \geq {}^5/_2$ for all $n \geq 6$.

(b): For the result from Theorem 11, one modifies the proof of Theorem 13 a bit. The underlying equation is now

$$(x + 3)^5 - (x - 3)^5 - 30(x^2 + 9)^2 = -1944$$

and let y be the product of 8 and all odd prime numbers between 5 and m, inclusively. Now one splits as in Theorem 13 the number -1944 into $a_4, a_5, \ldots, a_n$ what are $n-3$ odd coprime numbers which are all not multiples of a prime below 50 and where without loss of generality m was chosen so large that m is larger than any of the numbers generated by this splitting. Note that these numbers $a_4, \ldots, a_n$ are fixed while a_1, a_2, a_3 depend on the choice of m, h, y, x. Now one let $x-3 = (y+3)^{(m+h)!+1}$ so that $x-3$ modulo p is 3 for all odd prime numbers between 5 and m. $x+3$ is 9 modulo p for these prime numbers. Furthermore, if $p > 50$ then x^2+9 is $6^2+9 = 45$ modulo p. So choosing a_1, a_2, a_3 as $(x+3)^5$, $-(x-3)^5$ and $-30(x^2+9)^2$, respectively, completes the choice. a_2 is a high power of a small number, but a_1 and a_3 contribute the radical approximately in order x^3 and these are required to be brought down. As y is 0 modulo 8 and $(m+h)!+1$ is an odd power, $x-3$ is 3 modulo 8 and $x+3$ is 1 modulo 8. Furthermore, x^2+9 is $36+9$ modulo 8 what can be simplied to 5 modulo 8. So both $x+3$ and x^2+9 are the sums of three squares in the rational integers and of the form -1 times a square in the Hamiltonian integers. This gives that the sequence of tuples $(a_1, a_2, \ldots, a_n)$ chosen in dependence of the parameter h witnesses that $Q_{H(\{1\},\emptyset,n)} \geq 10/3$. How to choose m exactly in dependence of $a_4, \ldots, a_n$ such that the telescope sum arguements work and to do this verification is left to the reader. □

Remark 29. Hurwitz [8] as well as Hardy and Wright [6] consider a set C of units and then define that two numbers x, y are associates iff there are units $c, d \in C$ with $x = cyd$; as c, d are multiplicatively invertable, this definition is symmetric for x and y: $c^{-1}xd^{-1} = y$. So one might ask whether one gets a type of unique factorisation if one chooses the right set of units C. In other words, whether the pathology mentioned at the beginning of this section can be overcome by enlarging C beyond $\{-1, 1, -\mathbf{i}, \mathbf{i}, -\mathbf{j}, \mathbf{j}, -\mathbf{k}, \mathbf{k}\}$.

The apporach of Hurwitz [8] is to enlarge the Hamiltonian integers by adding in halfintegers where all four coordinates must differ exactly by 1/2 from a rational integer. The resulting set of units has then 24 members, the eight units given above plus sixteen additional ones where every coordinate is either $-1/2$ or $1/2$. Using these units, Hurwitz achieved that every halfinteger is the product of up to two of units and a Hamiltonian integer, leaving the units to be the only halfintegers to be relevant [6, Theorem 371].

But also this larger set C does not avoid the problem that numbers might fail to have a unique factorisation in the Hamiltonian integers. Here a Hamiltonian integer x is a prime iff $x \neq 0$, x is not a unit and all factors of x are either associates of x or units; an equivalent statement is that the norm of x is a prime in the natural numbers. Thus every natural number prime p, which has norm p^2, is the product of two Hamiltonian integer primes, each with norm p.

The Jacobi Four Square Theorem, see Hirschhorn [7] for the exact statement and a short proof, implies that an odd prime number p in the natural numbers can be written in $8(p+1)$ ways as a sum of four squares, $p = q^2+r^2+s^2+t^2$, where q, r, s, t are rational integers. Thus the number p can be written in $8(p+1)$ ways as a product $(q+r\mathbf{i}+s\mathbf{j}+t\mathbf{k}) \cdot (q-r\mathbf{i}-s\mathbf{j}-t\mathbf{k})$ and so there are at least $8(p+1)$ different prime factors of p in the Hamiltonian integers of which each one, paired with another one, multiplies to p.

However, when picking one of these factorisations, there are at most $2 \cdot |C|^2$ other factorisations where at least one of the numbers is an associate of one of the numbers in the given factorisation, thus the amount of these is constant while the overall number of possible factorisations is $8(p+1)$. Therefore, when p is sufficiently large, that is, when $p > 2|C|^2$, there are two factorisations $x \cdot y = p$ and $x' \cdot y' = p$ where x and y are both not associates of any of x' and y'.

In other words, these factorisations cannot be unique and one has indeed to minimise the quality of number by going over the quality of all possible factoriations instead of searching for a unique prime factorisation which does not exist, even not modulo associates. This result is then also independent on whether one uses eight units (as we do) or twentyfour units (as Hurwitz [8] and Hardy and Wright [6] do).

7 Conclusion

We first summarise our results. We showed that for all $n \geq 6$ and all finite sets $F \subseteq \{3, 4, 5, 6, \ldots\}$ that $Q_{U(\{1\},F,n)} \geq 5/4$. Furthermore, methods in principle known to the researchers in the field give for all odd n, $Q_{U(\{1\},\emptyset,n)} \geq 5/3$. For $n = 5$, we showed that for all finite sets $F \subseteq \{3, 4, 5, 6, \ldots\}$ there is a number $q_F > 1$ such that $Q_{U(\{1\},F,5)} \geq q_F$ but we were not able to find a common lower bound for all these q_F other than 1. In the case of the Gaussian integers, we were able to establish that for all $n \geq 4$ and all finite sets F of Gaussian integers which contain neither a unit nor $1 + \mathbf{i}$ multiplied with a unit, the lower bound $Q_{C(\{1\},F,n)} \geq 5/3$ holds.

The methods in the present work use polynomial identities. Mason [10] and Stother [17] proved that given a polynomial identity of the form $f + g = h$ where these functions are coprime as polynomials and not all of the functions are constant, the maximum degree of f, g, h is at most the number of distinct complex roots of $f \cdot g \cdot h$ minus 1. Known methods to choose the variable of the polynomial identity allow only to overcome the gap of 1 in the degrees, but they do not allow anything better; so one arrives at families of examples constructed with polynomial identities to have at most the guaranteed quality 1.

Furthermore, whenever a polynomial formula of three terms f, g, h in one variable produces more examples than its degree than the formula then the equality $f + g = h$ must hold, thus the above restriction applies. Thus solutions of formulas of the form $f + g = h$ which are parameterised by only one variable are not interesting. However, for several variable, this restriction of the Theorem of Mason and Stother does not apply, so the Pell equaltion $x^2 - z^3y^2 = 1$ has for each z which is not a perfect square infinitely many solutions. But the Theorem of Mason and Stoher says now that one cannot find parameterisations of x, y, z in one variable t which find infinitely many triples $(x(t), y(t), z(t))$ with $x(t)^2 - y(t)^2z(t)^3 = 1$.

The conjecture that the constant of the abc-conjecture is 1 implies a further restriction to such solutions (x, y, z), also when not parameterised by one variable: For an infinite sequence of solutions (x_k, y_k, z_k) with $x_k \to \infty$, the ratio $\log(z_k)/\log(x_k)$ must go to 0. This constraint does not come from the Theorem of Mason and Stother but is an additional constraint which is unproven.

Furthermore, for small numbers, researchers found examples of larger quality, as often some powers go in which do not stem from the polynomial identity; however, such effects require

exhaustive search to find and methods to utilise them systematically are not known. Therefore the methods here do not give any insights for the case $n = 3$. Shapiro and Sparer [15] generalised the Theorem of Mason and Stother to larger n but there a factor $n - 2$ goes into the equation which then permits the use of polynomial identities to construct the examples in this paper systematically. Furthermore, for $n = 4$, all known useful polynomial identities in the integers have two terms with factor 2, thus they do not apply; only for the Gaussian integers a useful polynomial identity is found by Elkies [4] which was utilised in Theorem 20 and then generalised to the full result using solutions to Pell equations. Therefore, for the rational integers, the lower bounds for $n = 3$ and $n = 4$ are still both 1; similarly for Gaussian integers, the lower bound for the case $n = 3$ is still 1. For all these constants, only lower bounds are known and any information on upper bounds is missing; so proven any upper bound is an important challenge and the overall goal would be to identify for interesting choices of E, F, n the value $Q_{U(E,F,n)}$.

The role of the exception set E and the forbidden set F is another source of research questions. For instance, let

$$Q_n = \sup\{Q_{U(E,F,n)} \colon \ E, F \subset \mathbb{N} \text{ finite}, \ 1 \in E, \ \min F \geq 3, \ E \cap F = \emptyset \text{ and } \#U(E,F,n) = \infty\}.$$

Then we can ask the following question.

Open Problem 30. *Are all Q_n bounded by some common constant c from above?*

Furthermore, the lower bounds obtained for the *abc*-conjecture and the strong *abc*-conjecture for Hamiltonian integers differ by a factor 2. This is mainly due to the fact that in the Hamiltonian integers, a setwise coprime sum of three numbers can have that the factors of the first two numbers are essentially the same, a phenomenon which does not occur in rational and Gaussian integers. Therefore the following question is natural to ask.

Open Problem 31. *Are the constants of the strong abc-conjecture and the normal abc-conjecture (= 3-conjecture) different in the Hamiltonian integers?*

The following table gives an overview of the currently known lower bounds; the n in the last two columns are at least 5.

Integer-Type, Conjecture-Type	Formula	3	4	5	6	odd n	even n
Rational integers, strong n-conjecture	$Q_{U(\{1\},\emptyset,n)}$	1	1	$5/3$	$5/4$	$5/3$	$5/4$
Gaussian integers, strong n-conjecture	$Q_{C(\{1\},\emptyset,n)}$	1	$5/3$	$5/3$	$5/3$	$5/3$	$5/3$
Hamiltonian integers, strong n-conjecture	$Q_{H(\{1\},\emptyset,n)}$	2	2	$10/3$	$5/2$	$10/3$	$5/2$
Hamiltonian integers, n-conjecture	$Q_{H'(\emptyset,n)}$	4	12	20	28	$8n$-20	$8n$-20

We do not claim that the new lower bounds are optimal, but we conjecture that all the constants here can be matched by some upper bounds, though these might be larger. We would like to thank Benne de Weger for correspondence and for making his unpublished notes available to us [22].

References

1. Jerzy Browkin. The *abc*-conjecture. *Number Theory*, pages 75–105, Hindustan Book Agency, 2000.
2. Jerzy Browkin and Juliusz Brzeziński. Some remarks on the *abc*-conjecture. *Mathematics of Computation*, American Mathematical Society, 62(206):931–939, 1994.
3. Henri Cohen. *Number Theory — Volume 1: Tools and Diophantine Equations.* Springer, 2007.
4. Henri Darmon and Andrew Granville. On the equations $z = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bulletin of the London Mathematical Society*, 27(6):513–543, 1995.
5. Johann Dirichlet. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin*, 48:51–71, 1837.
6. Godfrey Harold Hardy and Edward Maitland Wright. *An Introduction to the Theory of Numbers.* Fifth Edition, Oxford, Clarendon Press, 1979.
7. Michael D. Hirschhorn. A simple proof of the Jacobi's four-square theorem. *Proceedings of the American Mathematical Society*, 101(3):436–438, 1987.
8. Adolf Hurwitz. *Vorlesungen über Zahlentheorie und Quaternionen.* Springer Verlag, 1919. Reviewed at https://zbmath.org/?format=complete&q=an:47.0106.01.
9. Hendrik Willem Lenstra, Jr. Solving the Pell Equation. *Notices of the American Mathematical Society*, 49(2):182–192, 2002.
10. R. C. Mason. Equations over function fields. *Number Theory*, Noordwijerhout 1983, Proceedings of the Journées Arithmétiques. Springer *Lecture Notes in Mathematics* 1068:149–157, 1984.
11. David Masser. Open Problems. *Proceedings of the Symposium on Analytic Number Theory.* Imperial College London, 1985.
12. Joseph Oesterlé. Nouvelles approaches du "Théorème" de Fermate. *Astérisque*, 161–2:165–186, 1988.
13. Carl Pomerance. Computational number theory. *Princeton Companion to Mathematics*, pages 348–362, Princeton University Press, 2008.
14. Coen Ramaekers. The *abc*-conjecture and the *n*-conjecture. Bachelor Thesis. Eindhoven University of Technology, 2009. Available at https://pure.tue.nl/ws/portalfiles/portal/67739846/657782-1.pdf.
15. Harold N. Shapiro and Gerson H. Sparer. Extension of a Theorem of Mason. *Communications on Pure and Applied Mathematics*, 45(5):711–718, 1994.
16. Peter Shiu. The three-square theorem of Gauss and Legendre. *The Mathematical Gazette*, Cambridge University Press, 104(560):209-214, 2020.
17. W. Wilson Stothers. Polynomial identities and Hauptmoduln. *Quarterly Journal of Mathematics*, 32(3):349–370, 1981.
18. Paul Vojta. Diophantine Approximations and Value Distribution Theory. *Lecture Notes in Mathematics*, Springer, 1987.

19. Paul Vojta. A more general abc conjecture. *International Mathematics Research Notices*, Oxford Academic, 1998(21):1103–1116, 1998.
20. Michael Waldschmidt. Lecture on the *abc* conjecture and some of its consequences. *Springer PROMS* (Proceedings in Mathematics and Statistics) 98:211–230, 2015.
21. Stan Wagon. *Mathematica in action*. First edition, WH Freeman, 1991. Second edition, Springer Science and Business Media, New York, 1999.
22. Benne de Weger. Experiments on variants of the abc-conjecture. Manuscript, 2020.