Lower Bounds for the Strong N-Conjecture

Aquinas Hobor, Singapore
Rupert Hölzl, Munich
Elaine Li, Singapore
Tianyu Liu, Singapore
Frank Stephan, Singapore
Starting Examples

Sometimes one can make additive equations of integers such that, compared to the size, there are only few distinct prime factors.

- \(125 + 3 = 128\): Primefactors \(2, 3, 5\); radical 30.
- \(1024 + 5 = 1029\): Primefactors \(2, 3, 5, 7\); radical 210.
- \(2400 + 1 = 2401\): Primefactors \(2, 3, 5, 7\); radical 210.
- \(8181 + 11 = 8192\): Primefactors \(2, 3, 11, 101\); radical 6666.

**Radical of Example**: Smallest number such that every member of the sum divides some power of it; alternatively, largest square-free divider of the product of all terms in the sum.

**Quality of Example**: \(\log(\text{largest number})/\log(\text{radical})\). This value should be large.
The N-Conjecture

Requirements for Examples

- No common prime factors of all numbers, so
  \[1024 - 512 - 256 - 256 = 0\] is forbidden.

- Sum is zero: \[a_1 + a_2 + \ldots + a_n = 0\].

- No nontrivial subsums are zero: If \[\sum a_k \cdot b_k = 0\] and all \[b_k \in \{0, 1\}\] then \[b_k = 0\] for either all or no \(k\).

Let \(A(n)\) be the set of all these examples in the integers for given \(n\). Let \(Q_{A(n)}\) be the limit superior of the qualities of any one-one enumeration of the tuples in \(A(n)\).

The abc-conjecture by David Masser (1985) and Joseph Oesterlé (1988). \(Q_{A(3)} = 1\).

The \(n\)-conjecture by Jerzy Browkin and Juliusz Brzeziński (1994). For every \(n \geq 3\), \(Q_{A(n)} = 2n - 5\).
The Strong N-Conjecture

Requirements for Examples

- No common prime factors of any two numbers, so $9216 - 8192 - 1029 + 5 = 0$ is forbidden.
- Sum is zero: $a_1 + a_2 + \ldots + a_n = 0$.
- No nontrivial subsums are zero: If $\sum a_k \cdot b_k = 0$ and all $b_k \in \{0, 1\}$ then $b_k = 0$ for either all or no $k$.

Let $B(n)$ be the set of all these examples satisfying the first and second condition and $R(n)$ be the set of all examples satisfying all three conditions for given $n \geq 3$.

The Strong N-Conjecture.
(Browkin 2000): $Q_{B(n)} < \infty$ for all $n$.
(Ramaekers 2009, Wikipedia): $Q_{R(n)} = 1$ for all $n$.

Konyagin (see Browkin 2000): $Q_{B(n)} \geq 3/2$ for all odd $n \geq 5$; $Q_{R(5)} \geq 3/2$ (follows from proof immediately).
Setting of Present Work

Let $E, F$ be finite sets of numbers with $1 \in E$ and $\min(F) \geq 3$. Now $U(E, F, n)$ contains all tuples $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$ satisfying the following conditions:

- If $i \neq j$ then $\gcd(a_i, a_j) \in E$;
- $\sum a_k = 0$;
- If $\sum a_k \cdot b_k = 0$ and all $b_k \in \{-1, 0, 1\}$ then $b_k = 0$ for either all or no $k$;
- No member of $F$ divides any $a_k$.

Now note that $Q_{U(\{1\}, F, n)} \leq Q_{R(n)} \leq Q_{B(n)}$ for all $n \geq 3$.

$Q_{U(\{1, 2\}, \emptyset, 4)} \geq 3/2$ by the following polynomial identity of Daniel Davies: $(x^m + 2)^3 - x^{3m} - 6(x^m + 1)^2 - 2 = 0$; here one can take $m$ to be a large odd number and $x$ to be 5.
Main Results

Theorems

1. $Q_{U(\{1\}, \emptyset, n)} \geq 5/3$ for odd $n \geq 5$.

2. For any $F$ there is a constant $r > 1$ with $Q_{U(\{1\}, F, 5)} \geq r$.

3. For any $n \geq 6$ and any $F$, $Q_{U(\{1\}, F, n)} \geq 5/4$.

For the Gaussian integers (also known as complex integers), one can define similar notions leading to a notion $C(E, F, n)$ and one obtains the following:

4. For any $n \geq 4$ and any $F$ neither containing units nor fourth roots of $-4$, $Q_{C(\{1\}, F, n)} \geq 5/3$. 

Lower Bounds for the Strong N-Conjecture – p. 6
**Arbitrary Forbidden Sets**

**Theorem.** Let $F$ be a finite set with $\min(F) \geq 3$, $E = \{1\}$ and $n \geq 6$. Then $Q_{U(E,F,n)} \geq \frac{5}{4}$.

**Construction.** Let $y$ be the product of all members of $F \cup \{2, 3, 5, 7, 11, s\}$. Later $x$ is chosen as $(y + 1)^k$ for suitable $k$. Now let

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

Here a sideconstraint is that $10 \cdot y - 1$ is a prime; this can be obtained by choosing $s > \max(F \cup \{11\})$ accordingly.

- $-a_7, -a_8, \ldots, -a_n$ are odd prime numbers such that $|3a_k| < |a_{k+1}|$ for $k = 7, 8, \ldots, n - 1$ and $|a_7| > 300y^6$. 

Lower Bounds for the Strong N-Conjecture – p. 7
Choosing the last two numbers

Now one chooses \( a_5 \) and \( a_6 \) such that (a) they are coprime to all other numbers and (b) their sum is
\[
u = -(a_1 + a_2 + a_3 + a_4 + a_7 + \ldots + a_n)
\]
This makes the sum of all \( a_k \) to be directly 0.

One first let \( q \) be the product of all primes below
\[
300 \cdot \max\{ |y|^6, |a_7|, |a_8|, \ldots, |a_n| \}.
\]

1. Let \( v = u + 1 + q \) and \( w = -q - 1 \).

2. For all odd prime numbers \( p \) dividing \( q \) Do

3. \{ While \( p \) divides one of \( v \) or \( w \)

    Do \{ \( v = v + q/p \) and \( w = w - q/p \) \} \}

4. If 4 divides \( v \) then let \( v = v + q \) and \( w = w - q \).

Then let \( a_5 = v \) and \( a_6 = w \).
Choosing \( k \)

Now \( k \) is chosen such that it is \( h! \) for a \( h \) larger than the absolute values of all of \( a_5, a_6, \ldots, a_n \).

Any prime factor \( p \) of \( a_5, \ldots, a_n \) satisfies that \( x = (y + 1)^k \) is 0 or 1 modulo \( p \); as the prime factor \( p \) is at least \( 300y^6 \), \( x \) is actually 1 modulo \( p \). \( a_1 \) and \( a_2 \) are \((y + 1)^5\) and \((y - 1)^5\) modulo \( p \). \( a_3 \) is \(-(10 \cdot y - 1)\) modulo \( p \). \( a_4 \) is \((1 + 10y^3)^2\) modulo \( p \). As \( p > 300y^6 \), \( p \) does not divide any of these numbers. \( a_5, \ldots, a_n \) are prime relative to each other. One can also verify that \( a_1, \ldots, a_4 \) are prime to each other: As \( x \) is coprime to \( y \) and \( y \) is even, \( x, x + y, x - y \) are all coprime to each other; also as \( 10y - 1 \) is a prime and \( x \) is 1 modulo \( 10y - 1 \), \( a_1 \) and \( a_2 \) are coprime to \( 10y - 1 \) and thus to \( a_3 \). Similarly one verifies that \( a_4 \) is coprime to \( a_1, a_2, a_3 \).
Determining the Quality

For the quality of this family of examples, note that $y$ and $a_5, \ldots, a_n$ are constants in the family while one is varying the exponent $k = h!$ in the expression $x = (y + 1)^k$. The factors $(x + y)^5$, $-(x - y)^5$ and $-(x^2 + 10y^3)$ contribute to the radical either the factors $x + y$, $x - y$ and $x^2 + 10y^3$ or some proper factors of these; furthermore, $-(10y - 1) \cdot x^4$ contributes to the radical either $(10y - 1) \cdot (y + 1)$ or a factor of that what is $O(1)$, as $y$ is constant independent of $x$. The numbers $a_5, \ldots, a_n$ are also constants independent of $x$ and contribute to the radical only size $O(1)$. Furthermore, $(x + y)$ is the largest term in the sum. So the quality is

$$5 \cdot \frac{\log(O(x))}{\log(O(x) \cdot O(x) \cdot O(x^2) \cdot O(1))}$$

which converges to $5/4$ for larger and larger values of $h$ and $x = (y + 1)^{h!}$. 

Lower Bounds for the Strong N-Conjecture – p. 10
The Case \( N = 5 \)

**Theorem.** Let \( E, F \) be finite sets with \( 1 \in E \) and \( 2, 5, 7, 10 \notin F \). Then \( Q_{U(E,F,5)} \geq 5/3 \).

**Construction.** Let \( y = (\max(F \cup \{11\}))!, \) \( k \) a large integer and \( x = (y + 1)^k - 1 \). The sum

\[
(x + 1)^5 - (x - 1)^5 - 10(x^2 + 1)^2 - 7 - 1 = 0
\]

and the terms in the sum have at least the quality

\[
5 \cdot \log(x + 1) / \log(7 \cdot (y + 1) \cdot (x - 1) \cdot (x^2 + 1))
\]

The coprimeness follows from the fact that \( x + 1, x - 1, x^2 + 1 \) are coprime and that all primes up to 11 are factors of \( y \) and \( y \) is a factor of \( x \). The subsum condition is easy to verify.

The result holds also for all odd \( n \geq 7 \).
Case N=5 and Arbitrary F

Theorem. Let $F$ be finite and $\min(F) \geq 3$. Then $Q_{U(\{1\}, F, 5)} > 1$.

Ramaekers (2009) mentioned a construction for four numbers which will here be slightly modified and the last will be split into two numbers.

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

Lower Bounds for the Strong N-Conjecture – p. 12
Here $p$ is $h! - 1$ for some $h$ larger than all members of $F$. One can compute the values of $a_1 + a_2 + a_3$ modulo $x^2, x^2 - 1, x^2 + (p - 1)/2$ which turn out to be numbers and not polynomials, as $a_1 + a_2 + a_3$ is an even polynomial in $x$ of degree $p - 5$. One chooses $y$ such that neither $y$ nor the sum of $y$ with any of the three remainders will be a multiple of any member of $F$. Furthermore, one chooses $x$ to be a large factorial. The quality of the example is approximately

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

which is approximately $p/(p - 1)$; note that $y$ is constant when choosing $x$. 

Proof Continued
Coen Ramaekers (2009) discussed a polynomial identity which allows to have $Q_{U(\{1,2\},\emptyset,4)} \geq \frac{5}{3}$; this identity is

$$(x + 1)^5 - (x - 1)^5 - 10 \cdot (x^2 + 1)^2 + 8 = 0.$$ 

Furthermore, for larger but still finite sets $E$ one can show $Q_{U(E,\emptyset,5)} \geq \frac{7}{4}$ and $Q_{U(E,\emptyset,5)} \geq \frac{9}{5}$. The polynomial identities are

$$(x + 1)^7 - (x - 1)^7 - 14(x^2 + 1)^3 - 28x^4 + 12 = 0$$

with $E = \{1, 2, 4, 7, 14\}$ and

$189(x+1)^9 - 189(x-1)^9 - 42(3x^2+7)^4 + 16(63x^2+79)^2 + 608 = 0$

with $E \subseteq \{1, 2, 3, \ldots, 608\}$. 
Gaussian Integers

The Gaussian integers are integers of the form \( a + b\sqrt{-1} \) and they have a norm \( a^2 + b^2 = (a + b\sqrt{-1}) \cdot (a - b\sqrt{-1}) \). The primes of integers can sometimes be factorised further, so one gets the following unusual factorisation examples:

\[
-4 = (1 + \sqrt{-1})^4 \quad \text{and} \quad 5 = (2 + \sqrt{-1}) \cdot (2 - \sqrt{-1})
\]

One can define the set \( \mathbb{C}(E, F, n) \) analogously to the case of the integers, with the following quality definition:

\[
q(a_1, \ldots, a_n) = \frac{\log(\max\{|a_1|, \ldots, |a_n|\})}{\log(|\text{rad}(a_1 \cdot \ldots \cdot a_n)|)}
\]

Here \( |a_k| \) is the square-root of the norm; the above equation would also work, if one replaces the absolute value by the norm everywhere. Primes \( p, -p, p \cdot \sqrt{-1}, -p \cdot \sqrt{-1} \) are equivalent; only one of them can go into the radical.

\( F \) does not contain any fourth root of \(-4\), but can contain \( 2 \).
Towards a Result 1

Noam D. Elkies (Darmon and Granville 1995) provided the following polynomial identity:

\[
(x^2 + 2 \cdot x \cdot y - 2 \cdot y^2)^5 - (x^2 - 2 \cdot x \cdot y - 2 \cdot y^2)^5 + \\
\sqrt{-1} \cdot (-x^2 + \sqrt{-1} \cdot 2 \cdot x \cdot y - 2 \cdot y^2)^5 - \\
\sqrt{-1} \cdot (-x^2 - \sqrt{-1} \cdot 2 \cdot x \cdot y - 2 \cdot y^2)^5 = 0.
\]

One can show that a common prime factor of any two of these numbers is a factor of either \(x\) or \(2y\). Furthermore, \(x^2 - 2xy - 2y^2 = (x - y)^2 - 3y^2\) and one can use Pell equations to set this to 1: \(x - y = v, y = uw\) where \(u\) can be chosen freely and \(v, w\) solve \(v^2 - (3u^2)w^2 = 1\). Now \(y = uw\) and \(x = v + uw\). As \(uw, v\) have the greatest common divisor 1, so do \(v + uw\) and \(uw\), thus \(x\) and \(y\). Now one can see that no divisor of \(x\) or \(y\) divides any of the four terms in the above polynomial identity.
Towards a Result 2

By letting \( u \) be the product of all norms of Gaussian integers in a finite set \( F \), one can achieve that all prime factors of numbers in \( F \) divide \( y \) and thus none of the four terms is divided by them.

Now there are three fifth powers of similarly large terms plus one term of value \(-1\) in the sum. Thus the radical is bounded by the third power of the largest term \( z \) and so the quality is at least \( 5 \cdot \log(z) / 3 \cdot \log(z) = 5/3 \).

These arguments can be generalised to all \( n \geq 4 \) giving the following theorem, provided that \( F \) does not contain any fourth root of \(-4\).

Theorem. \( Q_{C({1},F,n)} \geq 5/3 \) for all \( n \geq 4 \).
Example

Now \( z_0 = 3650401 \) and \( y_0 = 2107560 \) satisfy \( z_0^2 - 3y_0^2 = 1 \). Furthermore, \( y_0 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 193 \). Thus Elkies’ equation with \( y_0 \) and \( x_0 = y_0 + z_0 \) provides an example for \( n = 4 \) with \( F \) containing 3, 5, 7 and their factors. One gets further examples by

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

and then one can use that in Elkies equation the second term is \(-1\) and replace it by \(-3 - 5 + 7\) to get the following equation

\[
(x^2 + 2 \cdot x \cdot y - 2 \cdot y^2)^5 - 3 - 5 + 7 + \\
\sqrt{-1} \cdot (-x^2 + \sqrt{-1} \cdot 2 \cdot x \cdot y - 2 \cdot y^2)^5 - \\
\sqrt{-1} \cdot (-x^2 - \sqrt{-1} \cdot 2 \cdot x \cdot y - 2 \cdot y^2)^5 = 0
\]

to witness \( Q_C(\{1\}, \emptyset, 6) \geq 5/3 \) with the above sequence of \( (x_n, y_n, z_n) \).
This paper has no results for the case \( n = 3 \). The reason is that polynomial identities do not work here and there is even a theorem stating the reason.

**Theorem [Mason (1983) and Stother (1981)]**. If \( p + q = r \) is a polynomial identity of coprime polynomials in \( \ell \) variables and \( r \) is not constant then

\[
\deg(\text{rad}(p \cdot q \cdot r)) \geq \max\{\deg(p), \deg(q), \deg(r)\} + \ell.
\]

Such methods give usually

\[
\text{quality} \geq \frac{\deg(\text{largest term})}{\deg(\text{radical}) - \ell}.
\]

Furthermore, for the normal integers, no useful polynomial identities are known for \( n = 4 \) where all coefficients are odd.
However, computer search provided lots of examples of good quality, the best have qualities 1.6299 (Eric Reyssat, $2 + 3^{10} \cdot 109 = 23^5$), 1.6260 (Benne de Weger, $11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$) and 1.6235 (Jerzy Browkin, Juliusz Brzezinski, $19 \cdot 1307 + 7 \cdot 29^2 \cdot 31^8 = 2^8 \cdot 3^{22} \cdot 5^4$). Benne de Weger also found the largest known so far example with radical 210; it has quality 1.5679 and is $1 + 2 \cdot 3^7 = 5^4 \cdot 7 = 4375$. For extremely large numbers, one bumps up smaller examples at the expense of quality.

For $m = 8, 9, \ldots, 18$, one got for each $m$ between 10 and 17 examples of 3-tuples with largest number having $m$ decimal digits and quality at least 1.4 by exhaustive search. So perhaps the limit quality is, for $n = 3$, at least 1.4.

Coen Ramaekers was student of Benne de Weger and did calculations for the strong $n$-conjecture with $n \in \{4, 5\}$. 
Summary

The talk summarised the knowledge about the strong $n$-conjecture and advocated that one reexamines the bound conjectured there. Lower bounds of $\frac{5}{3}$ for odd $n \geq 5$ and $\frac{5}{4}$ for even $n \geq 6$ were obtained; however, Ramaekers original bound of $1$ was not improved for $n = 3$ and $n = 4$.

For the complex version of the strong $n$-conjecture, a uniform lower bound of $\frac{5}{3}$ was given for all $n \geq 4$.

It is conjectured that there is a uniform upper bound for all $Q_{U(E,F,n)}$ where $E$ is finite and that this bound is perhaps $2$.

All these bounds use a strong form of the avoidance of nontrivial subsums; Browkin (2000) citing Konyagin who did not consider the avoidance of subsums had already in the weaker version that odd $n \geq 5$ have the lower bound $\frac{3}{2}$. 