Lower Bounds for the Strong N-Conjecture

Aquinas Hobor, Singapore

Rupert Hölzl, Munich

Elaine Li, Singapore

Frank Stephan, Singapore

http://www.comp.nus.edu.sg/~fstephan/strongnconjecture.pdf

http://..../strongnconjectureslides.pdf

Starting Examples

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

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

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: $\log(\mathbf{largest\ number})/\log(\mathbf{radical})$. This value should be large.

The N-Conjecture

Requirements for Examples

- No common primefactors of all numbers, so $\mathbf{1024 - 512 - 256 - 256 = 0}$ is forbidden.
- Sum is zero: $\mathbf{a_1 + a_2 + \ldots + a_n = 0}$.
- No nontrivial subsums are zero: If $\sum \mathbf{a_k \cdot b_k = 0}$ and all $\mathbf{b_k \in \{0, 1\}}$ then $\mathbf{b_k = 0}$ for either all or no $\mathbf{k}$.

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

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

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

The Strong N-Conjecture

Requirements for Examples

- No common primefactors 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 $\mathbf{E}, \mathbf{F}$ be finite sets of numbers with $\mathbf{1} \in \mathbf{E}$ and $\min(\mathbf{F}) \geq \mathbf{3}$. Now $\mathbf{U}(\mathbf{E}, \mathbf{F}, \mathbf{n})$ contains all tuples $(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}) \in \mathbb{Z}^{\mathbf{n}}$ satisfying the following conditions:

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

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

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

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, $Q_{U(\{1\},F,n)} \geq 5/4$.

At Gaussian integers and Hamiltonian integers, notions $C(E, F, n)$ and $H(E, F, n)$ similar to $U(E, F, n)$ exist.

4. For any $n \geq 4$ and any F neither containing units nor fourth roots of -4, $Q_{C(\{1\},F,n)} \geq 5/3$.
5. $Q_{H(\{1\},\emptyset,3)} \geq 2$ and $Q_{H(\{1\},\emptyset,4)} \geq 2$;
6. $Q_{H(\{1\},F,n)} \geq 5/2$ for $n \geq 6$; $Q_{H(\{1\},\emptyset,n)} \geq 10/3$ for odd $n \geq 5$.
7. For $n \geq 3$, a lower bound of the n-conjecture in the Hamiltonian integers is $4 \cdot (2n - 5)$.

Arbitrary Forbidden Sets

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

Construction. Let $\mathbf{y}$ be the product of all members of $\mathbf{F} \cup \{\mathbf{2},\mathbf{3},\mathbf{5},\mathbf{7},\mathbf{11},\mathbf{s}\}$. Choose as $(\mathbf{y}+\mathbf{1})^{\mathbf{h}!}$ for large $\mathbf{h}$ and $\mathbf{a_1},\mathbf{a_2},\mathbf{a_3},\mathbf{a_4}$ with $\mathbf{a_1}+\mathbf{a_2}+\mathbf{a_3}+\mathbf{a_4} = -\mathbf{2y^5}+\mathbf{100y^6}$ by:

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

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

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

Choosing the last two numbers

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

One first let $\mathbf{q}$ be the product of all primes below $\mathbf{10 \cdot \max\{600 \cdot |y|^6, |a_7|, |a_8|, \ldots, |a_n|\}}$.

1. Let $\mathbf{v = u + 1 + q}$ and $\mathbf{w = -q - 1}$.
2. For all odd prime numbers $\mathbf{p}$ dividing $\mathbf{q}$ Do
3. $\{$ While $\mathbf{p}$ divides one of $\mathbf{v}$ or $\mathbf{w}$
   Do $\mathbf{\{v = v + q/p}$ and $\mathbf{w = w - q/p\}\}}$.
4. If $\mathbf{4}$ divides $\mathbf{v}$ then let $\mathbf{v = v + q}$ and $\mathbf{w = w - q}$.

Then let $\mathbf{a_5 = v}$ and $\mathbf{a_6 = w}$.

Choosing h

Now $\mathbf{h}$ is chosen larger than the absolute values of all of $\mathbf{a_5, a_6, \ldots, a_n}$.

Any prime factor $\mathbf{p}$ of $\mathbf{a_5, \ldots, a_n}$ satisfies that $\mathbf{x = (y+1)^{h!}}$ is $\mathbf{0}$ or $\mathbf{1}$ modulo $\mathbf{p}$; as the prime factor $\mathbf{p}$ is at least $\mathbf{600y^6}$, $\mathbf{x}$ is actually $\mathbf{1}$ modulo $\mathbf{p}$. $\mathbf{a_1}$ and $\mathbf{a_2}$ are $\mathbf{(y+1)^5}$ and $\mathbf{(y-1)^5}$ modulo $\mathbf{p}$. $\mathbf{a_3}$ is $\mathbf{-(10 \cdot y - 1)}$ modulo $\mathbf{p}$. $\mathbf{a_4}$ is $\mathbf{(1+10y^3)^2}$ modulo $\mathbf{p}$. As $\mathbf{p > 600y^6}$, $\mathbf{p}$ does not divide any of these numbers. $\mathbf{a_5, \ldots, a_n}$ are prime relative to each other. One can also verify that $\mathbf{a_1, \ldots, a_4}$ are prime to each other: As $\mathbf{x}$ is coprime $\mathbf{y}$ and $\mathbf{y}$ is even, $\mathbf{x, x+y, x-y}$ are all coprime to each other; also as $\mathbf{10y-1}$ is a prime and $\mathbf{x}$ is $\mathbf{1}$ modulo $\mathbf{10y-1}$, $\mathbf{a_1}$ and $\mathbf{a_2}$ are coprime to $\mathbf{10y-1}$ and thus to $\mathbf{a_3}$. Similarly one verifies that $\mathbf{a_4}$ is coprime to $\mathbf{a_1, a_2, a_3}$.

Determining the Quality

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

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

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

The Case N = 5

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

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

$$(\mathbf{x}+\mathbf{1})^{\mathbf{5}} - (\mathbf{x}-\mathbf{1})^{\mathbf{5}} - \mathbf{10}(\mathbf{x}^{\mathbf{2}}+\mathbf{1})^{\mathbf{2}} - \mathbf{7} - \mathbf{1} = \mathbf{0}$$

and the terms in the sum have at least the quality

$$\mathbf{5} \cdot \log(\mathbf{x}+\mathbf{1}) / \log(\mathbf{7} \cdot (\mathbf{y}+\mathbf{1}) \cdot (\mathbf{x}-\mathbf{1}) \cdot (\mathbf{x}^{\mathbf{2}}+\mathbf{1}))$$

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

The result holds also for all odd $\mathbf{n} \geq \mathbf{7}$.

Gaussian and Hamiltonian Integers

Gauss (Complex integers): $\mathbf{x = q + r \cdot i}$ where $\mathbf{q, r} \in \mathbb{Z}$;
Hamilton: $\mathbf{x = q + r \cdot i + s \cdot j + t \cdot k}$ where $\mathbf{q, r, s, t} \in \mathbb{Z}$.

Rules: $\mathbf{i^2 = -1}$, $\mathbf{j^2 = -1}$, $\mathbf{k^2 = -1}$, $\mathbf{i \cdot j \cdot k = -1}$;
Product of different imaginary units anticommutative;
Product of integers with any number commutative.

Norm and Conjugate: $\mathbf{\bar{x} = q - r \cdot i - s \cdot j - t \cdot k}$ is conjugate of $\mathbf{x}$, $\mathbf{x \cdot \bar{x} = q^2 + r^2 + s^2 + t^2}$ is the norm.
Norms are multiplicative. If the norm is a prime number then the number is prime in Gaussian and Hamiltonian integers. In Gaussian integers, $\mathbf{3}$ has norm $\mathbf{9}$ but cannot be factorised, as $\mathbf{3}$ is not the sum of two integer squares. In the Hamiltonian integers, a natural number $\mathbf{x}$ is of the form $\mathbf{-1 \cdot y^2}$ iff $\mathbf{x}$ is the sum of three integer squares, that is, if $\mathbf{x}$ is not of the form $\mathbf{4^a \cdot (8b + 7)}$ (direct application of Legendre's Three Square Theorem).

Definitions

Factorisation and The Radnorm: A factorisation of $\mathbf{x}$ is a list of numbers such that their product is $\mathbf{x}$; a factorisation of a tuple $(\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n})$ is the concatination of factorisations of $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n}$ as lists. The radical of a factorisation is the listing out of the members of the factorisation without verbatim repetition.

Radnorm and Maxnorm: The maxnorm of a tuple is the largest norm of a member of the tuple. The radnorm is the smallest norm which is taken by some radical of a factorisation of a tuple.

Quality: The quality of a tuple $\mathbf{a} = (\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n})$ is $\mathbf{q}(\mathbf{a}) = \mathbf{maxnorm}(\mathbf{a})/\mathbf{radnorm}(\mathbf{a})$. A set $\mathbf{A} = \{\mathbf{a_1}, \mathbf{a_2}, \ldots\}$ of tuples has quality $\mathbf{Q_A} = \limsup_{\mathbf{m}=1,2,\ldots} \mathbf{q}(\mathbf{a_m})$. Furthermore, $\mathbf{C}(\mathbf{E}, \mathbf{F}, \mathbf{n}), \mathbf{H}(\mathbf{E}, \mathbf{F}, \mathbf{n})$ are the adjustments of $\mathbf{U}(\mathbf{E}, \mathbf{F}, \mathbf{n})$ to the Gaussian and Hamiltonian integers.

Gaussian and Hamiltonian Integers

Theorem. If $\mathbf{n} \geq \mathbf{4}$ then $\mathbf{Q_{C(\{1\},F,n)}} \geq \mathbf{5/3}$.

Theorem. If $\mathbf{a, b, c}$ are normal integers with $\mathbf{a + b = c}$ then $\mathbf{q(a, b, c)}$ in the Hamiltonian integers is between $\mathbf{q((a, b, c))}$ and $\mathbf{2q(a, b, c)}$ in the normal integers.

Theorem. $\mathbf{Q_{H(\{1\},F,n)}} \geq \mathbf{5/2}$ for $\mathbf{n} \geq \mathbf{6}$ by verifying that in $\mathbf{x + y, x - y, x^2 + 10y^3}$ are sums of three squares in that result and thus have roots in the Hamiltonian integers; $\mathbf{x}$ is a large power of $\mathbf{y + 1}$.

Theorem. The quality of the $\mathbf{n}$-conjecture in the Hamiltonian integers is at least $\mathbf{4 \cdot (2n - 5)}$, using a result that one can choose an odd $\mathbf{x}$ with $\mathbf{x + \bar{x} = 2}$ and $\mathbf{x, \bar{x}}$ having a joint large factor $\mathbf{y}$ occuring four times in the factorisations with all other factors being units.

The Problems of Small N

No results for the case $\mathbf{n = 3}$ for normal and Gaussian integers. 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 $\mathbf{p + q = r}$ is a polynomial identity of coprime polynomials in ℓ variables and $\mathbf{r}$ is not constant then

$$\mathbf{deg(rad(p \cdot q \cdot r)) \geq max\{deg(p), deg(q), deg(r)\} + \ell.}$$

Such methods give usually

$$\mathbf{quality \geq \frac{deg(largest\ term)}{deg(radical) - \ell}.}$$

Furthermore, for the normal integers, no useful polynomial identies are known for $\mathbf{n = 4}$ where all coefficients are odd.

Summary

The talk summarised the knowledge about the strong n-conjecture and advocated that one reexamines the bound conjectured there. Lower bounds of $5/3$ for odd $n \geq 5$ and $5/4$ 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 $5/3$ was given for all $n \geq 4$.

The lower bounds for the strong n-conjecture scale up by a factor 2 and for the n-conjecture by a factor 4 in the Hamiltonian integers.

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 $3/2$.

Case N=5 and Arbitrary F

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

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

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

Proof Continued

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

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

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

Nontrivial Exception Sets E

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

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

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

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

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

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

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

Gaussian Integers Result Part 1

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

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

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.

Gaussian Integers Result Part 2

By letting $\mathbf{u}$ be the product of all norms of Gaussian integers in a finite set $\mathbf{F}$, one can achieve that all prime factors of numbers in $\mathbf{F}$ divide $\mathbf{y}$ 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 $-\mathbf{1}$ in the sum. Thus the radical is bounded by the third power of the largest term $\mathbf{z}$ and so the quality is at least $\mathbf{5} \cdot \log(\mathbf{z})/\mathbf{3} \cdot \log(\mathbf{z}) = \mathbf{5/3}$.

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

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

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

$$\begin{aligned}
&(x^2 + 2 \cdot x \cdot y - 2 \cdot y^2)^5 - 3 - 5 + 7 + \\
&i \cdot (-x^2 + i \cdot 2 \cdot x \cdot y - 2 \cdot y^2)^5 - \\
&i \cdot (-x^2 - i \cdot 2 \cdot x \cdot y - 2 \cdot y^2)^5 = 0
\end{aligned}$$

to witness $Q_{C(\{1\},\emptyset,6)} \geq 5/3$ with the above sequence of (x_n, y_n, z_n).

Hamiltonian Integers - Examples

1. The Pell equation $a^2 - 2b^2 = 1$ can be generalised to $x^4 - 2y^4 = 1$ in the Gaussian integers, as one can find solutions (a, b) which are sum of three squares and so can be squared. This witnesses quality 2 for strong 3-conjecture.

2. One can choose $y = v + w \cdot i + w \cdot j$ with (a, b) as in 1 and has $y^2 = 1 + 2abi + 2abj$ and consider $x = y^2 \cdot -i \cdot y^2 \cdot i = 1 + 4abi - 8a^2b^2k$. $\bar{x} = -jxj$ and $x + \bar{x} = 2$. This witnesses quality 4 for 3-conjecture.

3. For x as in 2, one can show that $x^{2m+1} + \bar{x}^{2m+1} = \sum_{h=0,1,\ldots,m} c_h \cdot \mathrm{norm}(x)^h$ with $c_0 = 2^{m+1}$. Now x^{2m+1} and c_0 are coprime, for $m = n - 3$ there are n terms and degree $2m + 1 = 2n - 5$. These equations give the lower bound $4 \cdot (2n - 5)$ for the n-conjecture.

Equations for N-Conjecture

Let $\mathbf{z = norm(x)}$. One uses below recursive equation to compute concrete polynomials in $\mathbf{z}$; coefficients of even powers of $\mathbf{z}$ are positive and those of odd powers are negative; $\mathbf{x^{m+2} = 2x^{m+1} - \bar{x} \cdot x^{m+1} = 2x^{m+1} - z \cdot x^m}$.

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

Computer Search

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.

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 $\mathbf{5/3}$ for odd $\mathbf{n \geq 5}$ and $\mathbf{5/4}$ for even $\mathbf{n \geq 6}$ were obtained; however, Ramaekers original bound of $\mathbf{1}$ was not improved for $\mathbf{n = 3}$ and $\mathbf{n = 4}$.

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

The lower bounds for the strong $\mathbf{n}$-conjecture scale up by a factor $\mathbf{2}$ and for the $\mathbf{n}$-conjecture by a factor $\mathbf{4}$ in the Hamiltonian integers.

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 $\mathbf{n \geq 5}$ have the lower bound $\mathbf{3/2}$.