Digital expansions along arithmetic progressions

Lukas Spiegelhofer

TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

March 6, 2020, MU Leoben

The basic objects

- The binary expansion: every nonnegative integer n admits a unique expansion as a sum of pairwise different powers of 2:

$$n = \varepsilon_0 2^0 + \varepsilon_1 2^1 + \varepsilon_2 2^2 + \cdots ,$$

where $\varepsilon_i \in \{0, 1\}$.

- The Zeckendorf expansion: every nonnegative integer n admits a unique expansion as a sum of pairwise different, non-adjacent Fibonacci numbers defined by $F_0 = 0$, $F_1 = 1$, $F_{i+2} = F_i + F_{i+1}$:

$$n = \varepsilon_2 F_2 + \varepsilon_3 F_3 + \cdots ,$$

where $\varepsilon_i \in \{0, 1\}$ and $\varepsilon_{i+1} = 1 \Rightarrow \varepsilon_i = 0$.

The basic objects

- The binary expansion: every nonnegative integer n admits a unique expansion as a sum of pairwise different powers of 2:

  $$n = \varepsilon_0 2^0 + \varepsilon_1 2^1 + \varepsilon_2 2^2 + \cdots ,$$

  where $\varepsilon_i \in \{0, 1\}$.

- The Zeckendorf expansion: every nonnegative integer n admits a unique expansion as a sum of pairwise different, non-adjacent Fibonacci numbers defined by $F_0 = 0$, $F_1 = 1$, $F_{i+2} = F_i + F_{i+1}$:

  $$n = \varepsilon_2 F_2 + \varepsilon_3 F_3 + \cdots ,$$

  where $\varepsilon_i \in \{0, 1\}$ and $\varepsilon_{i+1} = 1 \Rightarrow \varepsilon_i = 0$.

The basic question

What happens to the digital (binary or Zeckendorf) expansion of n when we add a constant t?

- Let us begin with the binary case and $t = 1$. The (possibly empty) block of 1s on the right of the binary expansion of n is replaced by 0s, and the 0 to the left of the block is replaced by 1.

$$* \, 011 \cdots 1 \mapsto *100 \cdots 0 \tag{1}$$

- A similar thing happens for $t = 2$: the rightmost digit of n stays the same and (1) is applied for the remaining digits.
- For $t = 3$ we have the following cases:

$$*00 \mapsto *11; \qquad *01^k01 \mapsto *10^k00;$$

$$*01^k10 \mapsto *10^k01; \qquad *01^k11 \mapsto *10^k10.$$

The end?

- In this way, we can in principle describe the situation for any given t completely; anagously, this is the case for Zeckendorf.
- However, we obtain long case distinctions for growing t, and a structural principle describing these cases is unavailable. We do not fully understand digital expansions under addition, in particular, repeated addition—that is, along *arithmetic progressions*.
- An apparently simple, unsolved conjecture in this context is *Cusick's conjecture* on the *binary sum-of-digits function*: let $s(n)$ be the number of 1s in the binary expansion of n and let $t \geq 0$ be an integer. Is it true that, more often than not, we have $s(n+t) \geq s(n)$?
  In symbols, do we have $c_t > 1/2$, where

$$c_t = \lim_{N\to\infty} \frac{1}{N} \bigl|\{0 \leq n < N : s(n+t) \geq s(n)\}\bigr|?$$

- A related line of research concerns *short* arithmetic progressions. This will lead us to the notion *level of distribution*, which has a strong link to digital expansions of prime numbers.

The end?

- In this way, we can in principle describe the situation for any given t completely; anagously, this is the case for Zeckendorf.
- However, we obtain long case distinctions for growing t, and a structural principle describing these cases is unavailable. We do not fully understand digital expansions under addition, in particular, repeated addition—that is, along *arithmetic progressions*.
- An apparently simple, unsolved conjecture in this context is *Cusick's conjecture* on the *binary sum-of-digits function*: let $s(n)$ be the number of 1s in the binary expansion of n and let $t \geq 0$ be an integer. Is it true that, more often than not, we have $s(n+t) \geq s(n)$? In symbols, do we have $c_t > 1/2$, where

$$c_t = \lim_{N\to\infty} \frac{1}{N} \left|\{0 \leq n < N : s(n+t) \geq s(n)\}\right|?$$

- A related line of research concerns *short* arithmetic progressions. This will lead us to the notion *level of distribution*, which has a strong link to digital expansions of prime numbers.

The end?

- In this way, we can in principle describe the situation for any given t completely; anagously, this is the case for Zeckendorf.
- However, we obtain long case distinctions for growing t, and a structural principle describing these cases is unavailable. We do not fully understand digital expansions under addition, in particular, repeated addition—that is, along *arithmetic progressions*.
- An apparently simple, unsolved conjecture in this context is *Cusick's conjecture* on the *binary sum-of-digits function*: let $s(n)$ be the number of 1s in the binary expansion of n and let $t \geq 0$ be an integer. Is it true that, more often than not, we have $s(n+t) \geq s(n)$?
  In symbols, do we have $c_t > 1/2$, where
  $$c_t = \lim_{N \to \infty} \frac{1}{N} \bigl| \{0 \leq n < N : s(n+t) \geq s(n)\} \bigr| ?$$
- A related line of research concerns *short* arithmetic progressions. This will lead us to the notion *level of distribution*, which has a strong link to digital expansions of prime numbers.

The end?

- In this way, we can in principle describe the situation for any given t completely; anagously, this is the case for Zeckendorf.
- However, we obtain long case distinctions for growing t, and a structural principle describing these cases is unavailable. We do not fully understand digital expansions under addition, in particular, repeated addition—that is, along *arithmetic progressions*.
- An apparently simple, unsolved conjecture in this context is *Cusick's conjecture* on the *binary sum-of-digits function*: let $s(n)$ be the number of 1s in the binary expansion of n and let $t \geq 0$ be an integer. Is it true that, more often than not, we have $s(n+t) \geq s(n)$?
  In symbols, do we have $c_t > 1/2$, where
  $$c_t = \lim_{N\to\infty} \frac{1}{N} \bigl|\{0 \leq n < N : s(n+t) \geq s(n)\}\bigr|?$$
- A related line of research concerns *short* arithmetic progressions. This will lead us to the notion *level of distribution*, which has a strong link to digital expansions of prime numbers.

Section 1

Long arithmetic progressions

Densities for Cusick's conjecture

Let s be the binary sum-of-digits function.
For integers $t \geq 0$ and j we define the asymptotic densities

$$\delta(j, t) = \lim_{N \to \infty} \frac{1}{N} \bigl| \{0 \leq n < N : s(n+t) - s(n) = j\} \bigr|.$$

The condition $s(n+t) - s(n) = j$ is periodic with period $2^{\kappa(j,t)}$; therefore

$$\delta(j, t) = \lim_{N \to \infty} \frac{1}{N} \bigl| \{0 \leq \ell < N : s((\ell+1)t) - s(\ell t) = j\} \bigr|$$

for odd t (this holds for all $t \geq 0$, but $2 \nmid t$ is the interesting case).
Cusick's conjecture is therefore about *long arithmetic progressions*.

- The densities $\delta(j, t)$ give us a probability distribution on $\mathbb{Z}$ for each t.
- Clearly, $c_t = \delta(0, t) + \delta(1, t) + \delta(2, t) + \cdots$.

Densities for Cusick's conjecture

Let s be the binary sum-of-digits function.
For integers $t \geq 0$ and j we define the asymptotic densities

$$\delta(j,t) = \lim_{N\rightarrow\infty} \frac{1}{N} \bigl|\{0 \leq n < N : s(n+t) - s(n) = j\}\bigr|.$$

The condition $s(n+t) - s(n) = j$ is periodic with period $2^{\kappa(j,t)}$; therefore

$$\delta(j,t) = \lim_{N\rightarrow\infty} \frac{1}{N} \bigl|\{0 \leq \ell < N : s((\ell+1)t) - s(\ell t) = j\}\bigr|$$

for odd t (this holds for all $t \geq 0$, but $2 \nmid t$ is the interesting case).
Cusick's conjecture is therefore about *long arithmetic progressions*.

- The densities $\delta(j,t)$ give us a probability distribution on $\mathbb{Z}$ for each t.
- Clearly, $c_t = \delta(0,t) + \delta(1,t) + \delta(2,t) + \cdots$.

Densities for Cusick's conjecture

Let s be the binary sum-of-digits function.
For integers $t \geq 0$ and j we define the asymptotic densities

$$\delta(j,t) = \lim_{N\rightarrow\infty} \frac{1}{N} \bigl\lvert \{ 0 \leq n < N : s(n+t) - s(n) = j \} \bigr\rvert .$$

The condition $s(n+t) - s(n) = j$ is periodic with period $2^{\kappa(j,t)}$; therefore

$$\delta(j,t) = \lim_{N\rightarrow\infty} \frac{1}{N} \bigl\lvert \{ 0 \leq \ell < N : s((\ell+1)t) - s(\ell t) = j \} \bigr\rvert$$

for odd t (this holds for all $t \geq 0$, but $2 \nmid t$ is the interesting case).
Cusick's conjecture is therefore about *long arithmetic progressions*.

- The densities $\delta(j,t)$ give us a probability distribution on $\mathbb{Z}$ for each t.
- Clearly, $c_t = \delta(0,t) + \delta(1,t) + \delta(2,t) + \cdots$.

A two-dimensional recurrence

For $t = 1$, we have the rule $*01^k \mapsto *10^k$ valid for $k \geq 0$, therefore we have the geometric distribution

$$\delta(k,1) = \begin{cases} 0 & \text{for } k \geq 2; \\ 2^{k-2} & \text{for } k \leq 1. \end{cases}$$

$$\left(\begin{array}{c} \cdots \\ 0 \\ 0 \\ 1/2 \\ \hline 1/4 \\ \hline 1/8 \\ 1/16 \\ 1/32 \\ \cdots \end{array}\right)$$

It follows that $c_1 = 3/4 > 1/2$.

- We have the recurrence

$$\delta(j, 2t) = \delta(j, t);$$

$$\delta(j, 2t+1) = \frac{1}{2}\delta(j-1, t) + \frac{1}{2}\delta(j+1, t+1),$$

which permits to compute the values $\delta(j, t)$ efficiently. In particular, $c_t > 1/2$ for $t \leq 2^{30}$. ($\approx$ 2 CPU hours)

A two-dimensional recurrence

For $t = 1$, we have the rule $*01^k \mapsto *10^k$ valid for $k \ge 0$, therefore we have the geometric distribution

$$\delta(k,1) = \begin{cases} 0 & \text{for } k \ge 2; \\ 2^{k-2} & \text{for } k \le 1. \end{cases}$$

$$\left(\begin{array}{c} \dots \\ 0 \\ 0 \\ 1/2 \\ \hline 1/4 \\ \hline 1/8 \\ 1/16 \\ 1/32 \\ \dots \end{array}\right)$$

It follows that $c_1 = 3/4 > 1/2$.

- We have the recurrence

$$\delta(j, 2t) = \delta(j, t);$$

$$\delta(j, 2t+1) = \frac{1}{2}\delta(j-1, t) + \frac{1}{2}\delta(j+1, t+1),$$

which permits to compute the values $\delta(j,t)$ efficiently. In particular, $c_t > 1/2$ for $t \le 2^{30}$. (≈ 2 CPU hours)

An almost-all result

With this recurrence, it is not hard to compute the mean values

$$m_{\lambda,j} = \frac{1}{2^\lambda} \sum_{2^\lambda \le t < 2^{\lambda+1}} \delta(j,t).$$

It takes more effort to handle the second moment

$$m^{(2)}_{\lambda,j} = \frac{1}{2^\lambda} \sum_{2^\lambda \le t < 2^{\lambda+1}} \delta(j,t)^2.$$

Together with Drmota and Kauers, we studied $m^{(2)}$ by analyzing a *diagonal of a trivariate generating function* asymptotically. Using Chebychev's inequality, we obtained concentration strictly above 1/2!

Theorem (Drmota–Kauers–S. 2016)

For all $\varepsilon > 0$, we have

$$\left|\{0 \le t < T : 1/2 < c_t < 1/2 + \varepsilon\}\right| = T - \mathcal{O}\left(T/\log T\right).$$

An almost-all result

With this recurrence, it is not hard to compute the mean values

$$m_{\lambda,j} = \frac{1}{2^\lambda} \sum_{2^\lambda \le t < 2^{\lambda+1}} \delta(j,t).$$

It takes more effort to handle the second moment

$$m_{\lambda,j}^{(2)} = \frac{1}{2^\lambda} \sum_{2^\lambda \le t < 2^{\lambda+1}} \delta(j,t)^2.$$

Together with Drmota and Kauers, we studied $m^{(2)}$ by analyzing a *diagonal of a trivariate generating function* asymptotically. Using Chebychev's inequality, we obtained concentration strictly above $1/2$!

Theorem (Drmota–Kauers–S. 2016)

For all $\varepsilon > 0$, we have

$$\bigl|\{0 \le t < T : 1/2 < c_t < 1/2 + \varepsilon\}\bigr| = T - \mathcal{O}\left(T / \log T\right).$$

The Tu–Deng conjecture

Using similar methods, we (S.–Wallner 2019) proved an analogous almost-all result on the *Tu–Deng conjecture* coming from cryptography: for a positive integer k and $1 \le t < 2^k - 1$, this conjecture states that $|S_{t,k}| \le 2^{k-1}$, where

$$S_{t,k} = \Bigl\{0 \le a, b < 2^k - 1 : a + b \equiv t \bmod 2^k - 1, s(a) + s(b) < k\Bigr\}.$$

- This has been verified computationally for $k \in \{1, \ldots, 29, 39, 40\}$ by Tu and Deng, and Flori respectively.
- This conjecture, if true, allows for constructing Boolean functions $\{0,1\}^k \to \{0,1\}$ with desirable cryptographic properties.

The Tu–Deng conjecture

Using similar methods, we (S.–Wallner 2019) proved an analogous almost-all result on the *Tu–Deng conjecture* coming from cryptography: for a positive integer k and $1 \leq t < 2^k - 1$, this conjecture states that $|S_{t,k}| \leq 2^{k-1}$, where

$$S_{t,k} = \Bigl\{0 \leq a, b < 2^k - 1 : a + b \equiv t \bmod 2^k - 1, s(a) + s(b) < k\Bigr\}.$$

- This has been verified computationally for $k \in \{1, \ldots, 29, 39, 40\}$ by Tu and Deng, and Flori respectively.
- This conjecture, if true, allows for constructing Boolean functions $\{0,1\}^k \to \{0,1\}$ with desirable cryptographic properties.

The Tu–Deng conjecture

Using similar methods, we (S.–Wallner 2019) proved an analogous almost-all result on the *Tu–Deng conjecture* coming from cryptography: for a positive integer k and $1 \le t < 2^k - 1$, this conjecture states that $|S_{t,k}| \le 2^{k-1}$, where

$$S_{t,k} = \Big\{0 \le a, b < 2^k - 1 : a + b \equiv t \bmod 2^k - 1, s(a) + s(b) < k\Big\}.$$

- This has been verified computationally for $k \in \{1, \ldots, 29, 39, 40\}$ by Tu and Deng, and Flori respectively.
- This conjecture, if true, allows for constructing Boolean functions $\{0,1\}^k \to \{0,1\}$ with desirable cryptographic properties.

Current work

A promising different approach (started by Emme and Hubert) is to study moments of $\delta(\cdot, t)$ for fixed t. In this vein, we proved the following weakened form of the conjecture.

Theorem (S., submitted 2019)

Let $\varepsilon > 0$. If t contains at least $B(\varepsilon)$ blocks of 1s, then $c_t > 1/2 - \varepsilon$.

With Wallner, we are currently proving a stronger theorem:

Theorem (S., Wallner, in preparation)

Assume that K is the number of blocks of 1s in t. There exist (explicit) $\sigma \asymp K$ and $\alpha > 0$ such that for all $j \in \mathbb{Z}$,

$$\delta(j, t) = \alpha \exp\left(-\frac{j^2}{2\sigma}\right) + \mathcal{O}(K^{-1}).$$

In particular, $c_t > 1/2 - \mathcal{O}(K^{-1/2})$.

Current work

A promising different approach (started by Emme and Hubert) is to study moments of $\delta(\cdot, t)$ for fixed t. In this vein, we proved the following weakened form of the conjecture.

Theorem (S., submitted 2019)

Let $\varepsilon > 0$. If t contains at least $B(\varepsilon)$ blocks of 1s, then $c_t > 1/2 - \varepsilon$.

With Wallner, we are currently proving a stronger theorem:

Theorem (S., Wallner, in preparation)

Assume that K is the number of blocks of 1s in t. There exist (explicit) $\sigma \asymp K$ and $\alpha > 0$ such that for all $j \in \mathbb{Z}$,

$$\delta(j, t) = \alpha \exp\left(-\frac{j^2}{2\sigma}\right) + \mathcal{O}\big(K^{-1}\big).$$

In particular, $c_t > 1/2 - \mathcal{O}(K^{-1/2})$.

Current work

A promising different approach (started by Emme and Hubert) is to study moments of $\delta(\cdot, t)$ for fixed t. In this vein, we proved the following weakened form of the conjecture.

Theorem (S., submitted 2019)

Let $\varepsilon > 0$. If t contains at least $B(\varepsilon)$ blocks of 1*s, then $c_t > 1/2 - \varepsilon$.*

With Wallner, we are currently proving a stronger theorem:

Theorem (S., Wallner, in preparation)

Assume that K is the number of blocks of 1*s in t. There exist (explicit) $\sigma \asymp K$ and $\alpha > 0$ such that for all $j \in \mathbb{Z}$,*

$$\delta(j, t) = \alpha \exp\left(-\frac{j^2}{2\sigma}\right) + \mathcal{O}\left(K^{-1}\right).$$

In particular, $c_t > 1/2 - \mathcal{O}(K^{-1/2})$.

Current work, continued

This is proved by a detailed analysis of the *characteristic function* of $\delta(\cdot, t)$, viz.

$$\gamma_t(\vartheta) = \sum_{n \geq 0} e^{2\pi i \vartheta (s(n+t) - s(n))} = \sum_{j \in \mathbb{Z}} \delta(j, t) e^{2\pi i j \vartheta}.$$

For each ϑ, we have the *one-dimensional* recurrence

$$\begin{aligned} \gamma_1(\vartheta) &= \frac{\mathrm{e}(\vartheta)}{2 - \mathrm{e}(-\vartheta)}; \\ \gamma_{2t}(\vartheta) &= \gamma_t(\vartheta); \\ \gamma_{2t+1}(\vartheta) &= \frac{\mathrm{e}(\vartheta)}{2} \gamma_t(\vartheta) + \frac{\mathrm{e}(-\vartheta)}{2} \gamma_{t+1}(\vartheta). \end{aligned}$$

Probability theoretic tools are also powerful in this context!

Medium-term goals, part I

- Prove analogous results for the Tu–Deng conjecture.
- Prove the full sum-of-digits conjecture of Cusick. ☕ ☕
- Consider base-q analogues, and the *Zeckendorf sum-of-digits* of $n+t$!
- Consider multidimensional generalizations: prove that the densities

$$\delta(j_1,\ldots,j_m,t) = \lim_{N\to\infty}\frac{1}{N}\bigl|\{0\le n<N : s(n+\ell t)-s(n)=j_\ell \\ \text{for } 1\le \ell\le m\}\bigr|$$

define a probability distribution close to an m-variate Gaussian, and prove statements analogous to Cusick's conjecture.
Note that these are questions on *consecutive elements of long arithmetic progressions*.

Section 2

Short arithmetic progressions

An exponential sum

- We are interested in the exponential sum

$$\sum_{0 \le n < N} \mathrm{e}(\vartheta s(nt + a)),$$

  where $\mathrm{e}(x) = \exp(2\pi i x)$ and $\vartheta \in \mathbb{R}$, and we wish to obtain upper bounds.
- This allows us to prove statements on the distribution of $s(n) \bmod m$ along arithmetic progressions.
- Most prominently, we are concerned with the *Thue–Morse sequence* $\mathbf{t}$, which can be defined by $\mathbf{t}(n) = s(n) \bmod 2$, or by the morphism $0 \mapsto 01$, $1 \mapsto 10$. This corresponds to $\vartheta = 1/2$.

$$\mathbf{t} = (01101001100101101001011001101001\ldots)$$

  This sequence describes whether an even or an odd number of powers of two is needed to represent n (in the minimal representation).

An exponential sum

- We are interested in the exponential sum

$$\sum_{0\le n<N} \mathrm{e}(\vartheta s(nt+a)),$$

where $\mathrm{e}(x) = \exp(2\pi i x)$ and $\vartheta \in \mathbb{R}$, and we wish to obtain upper bounds.

- This allows us to prove statements on the distribution of $s(n) \bmod m$ along arithmetic progressions.
- Most prominently, we are concerned with the *Thue–Morse sequence* $\mathbf{t}$, which can be defined by $\mathbf{t}(n) = s(n) \bmod 2$, or by the morphism $0 \mapsto 01$, $1 \mapsto 10$. This corresponds to $\vartheta = 1/2$.

$$\mathbf{t} = (01101001100101101001011001101001\ldots)$$

This sequence describes whether an even or an odd number of powers of two is needed to represent n (in the minimal representation).

Gelfond's theorem

Theorem (Gelfond 1968)

Let $d \geq 1$ and $a \in \mathbb{Z}$. Then

$$\left|\{1 \leq n \leq x : \mathbf{t}(n) = 0, n \equiv a \bmod d\}\right| = \frac{x}{2d} + \mathcal{O}(x^{\lambda})$$

for some absolute λ.

- That is, for all $d \geq 1$ and $a < d$ we have

  $$\sum_{1 \leq m \leq M} (-1)^{s(md+a)} \ll M^{\lambda}.$$

  The implied constant depends on d (there are arbitrarily long APs on which $\mathbf{t}$ is constant!).
- Therefore we look at a certain average over d.

The level of distribution

Theorem (Fouvry–Mauduit 1996)

$$\sum_{1\le d\le D}\max_{1\le y\le x}\max_{0\le a<d}\left|\sum_{\substack{0\le n<y\\ n\equiv a \bmod d}}(-1)^{s(n)}\right|\le Cx^{1-\eta}$$

for some $\eta>0$ *and* $D=x^{0.5924}$.

- The number 0.5924 is a *level of distribution* of the Thue–Morse sequence.
- Note that we have "trivial" summands (of size $\asymp x/d$) for $d=2^\lambda+1$, where $x\le 2^{2\lambda}$. These don't matter in the sum.
- For d close to D, the APs have $x^{0.4076+\mathcal{O}(\eta)}$ many terms and common difference $\sim x^{0.5924}$. Note that $0.5924/0.4076\approx 1.453\rightarrow$ *short arithmetic progressions!*

The level of distribution

Theorem (Fouvry–Mauduit 1996)

$$\sum_{1\le d\le D}\max_{1\le y\le x}\max_{0\le a<d}\left|\sum_{\substack{0\le n<y\\ n\equiv a \bmod d}}(-1)^{s(n)}\right|\le Cx^{1-\eta}$$

for some $\eta>0$ *and* $D=x^{0.5924}$.

observed − expected

- The number 0.5924 is a *level of distribution* of the Thue–Morse sequence.
- Note that we have "trivial" summands (of size $\asymp x/d$) for $d=2^\lambda+1$, where $x\le 2^{2\lambda}$. These don't matter in the sum.
- For d close to D, the APs have $x^{0.4076+\mathcal{O}(\eta)}$ many terms and common difference $\sim x^{0.5924}$. Note that $0.5924/0.4076\approx 1.453\rightarrow$ *short arithmetic progressions!*

The level of distribution

Theorem (Fouvry–Mauduit 1996)

selects the "worst" AP

$$\sum_{1\le d\le D} \max_{1\le y\le x}\ \max_{0\le a<d}\left|\sum_{\substack{0\le n<y\\ n\equiv a \bmod d}} (-1)^{s(n)}\right| \le Cx^{1-\eta}$$

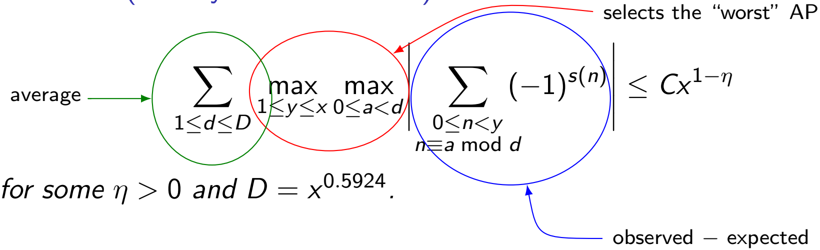
for some $\eta>0$ *and* $D=x^{0.5924}$.

observed − expected

- The number 0.5924 is a *level of distribution* of the Thue–Morse sequence.
- Note that we have "trivial" summands (of size $\asymp x/d$) for $d=2^\lambda+1$, where $x\le 2^{2\lambda}$. These don't matter in the sum.
- For d close to D, the APs have $x^{0.4076+\mathcal{O}(\eta)}$ many terms and common difference $\sim x^{0.5924}$. Note that $0.5924/0.4076\approx 1.453 \rightarrow$ *short arithmetic progressions!*

The level of distribution

Theorem (Fouvry–Mauduit 1996)



selects the "worst" AP

average

$$\sum_{1\le d\le D} \max_{1\le y\le x} \max_{0\le a<d} \left| \sum_{\substack{0\le n<y\\ n\equiv a \bmod d}} (-1)^{s(n)} \right| \le C x^{1-\eta}$$

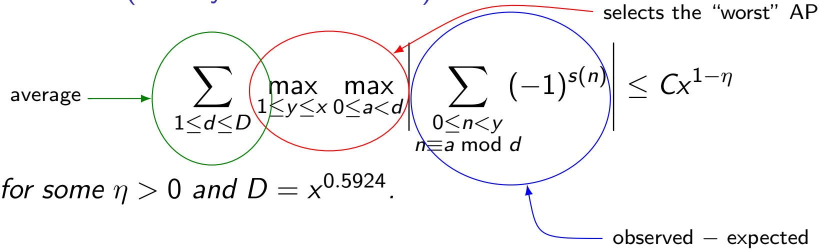
observed − expected

for some $\eta > 0$ *and* $D = x^{0.5924}$.

- The number 0.5924 is a *level of distribution* of the Thue–Morse sequence.
- Note that we have "trivial" summands (of size $\asymp x/d$) for $d = 2^\lambda + 1$, where $x \le 2^{2\lambda}$. These don't matter in the sum.
- For d close to D, the APs have $x^{0.4076+\mathcal{O}(\eta)}$ many terms and common difference $\sim x^{0.5924}$. Note that $0.5924/0.4076 \approx 1.453$ → *short arithmetic progressions!*

The level of distribution

Theorem (Fouvry–Mauduit 1996)



selects the "worst" AP

average

$$\sum_{1\le d\le D}\ \max_{1\le y\le x}\ \max_{0\le a<d}\left|\sum_{\substack{0\le n<y\\ n\equiv a \bmod d}}(-1)^{s(n)}\right|\le Cx^{1-\eta}$$

for some $\eta>0$ *and* $D=x^{0.5924}$.

observed − expected

- The number 0.5924 is a *level of distribution* of the Thue–Morse sequence.
- Note that we have "trivial" summands (of size $\asymp x/d$) for $d=2^\lambda+1$, where $x\le 2^{2\lambda}$. These don't matter in the sum.
- For d close to D, the APs have $x^{0.4076+\mathcal{O}(\eta)}$ many terms and common difference $\sim x^{0.5924}$. Note that $0.5924/0.4076\approx 1.453\to$ *short arithmetic progressions!*

The level of distribution

Theorem (Fouvry–Mauduit 1996)

selects the "worst" AP

average

$$\sum_{1 \le d \le D} \max_{1 \le y \le x} \max_{0 \le a < d} \left| \sum_{\substack{0 \le n < y \\ n \equiv a \bmod d}} (-1)^{s(n)} \right| \le C x^{1-\eta}$$

for some $\eta > 0$ *and* $D = x^{0.5924}$.

observed − expected

- The number 0.5924 is a *level of distribution* of the Thue–Morse sequence.
- Note that we have "trivial" summands (of size $\asymp x/d$) for $d = 2^\lambda + 1$, where $x \le 2^{2\lambda}$. These don't matter in the sum.
- For d close to D, the APs have $x^{0.4076+\mathcal{O}(\eta)}$ many terms and common difference $\sim x^{0.5924}$. Note that $0.5924/0.4076 \approx 1.453 \rightarrow$ *short arithmetic progressions!*

The level of distribution

Theorem (S., submitted 2018)

The Thue–Morse sequence has level of distribution 1*. More precisely, let* $0 < \varepsilon < 1$*. There exist* $\eta > 0$ *and* C *such that*

$$\sum_{1 \le d \le D} \max_{\substack{y,z \ge 0 \\ z-y \le x}} \max_{0 \le a < d} \left| \sum_{\substack{y \le n < z \\ n \equiv a \bmod d}} (-1)^{s(n)} \right| \le C x^{1-\eta}$$

for $D = x^{1-\varepsilon}$*.*

- This is a statement on *very short arithmetic progressions*: the Thue–Morse sequence usually shows cancellation along N-term arithmetic progressions having common difference $\sim N^R$, where $R > 0$ is arbitrary ($R \le 1.454$ for Fouvry–Mauduit).

The level of distribution

Theorem (S., submitted 2018)

The Thue–Morse sequence has level of distribution 1. *More precisely, let* $0 < \varepsilon < 1$. *There exist* $\eta > 0$ *and* C *such that*

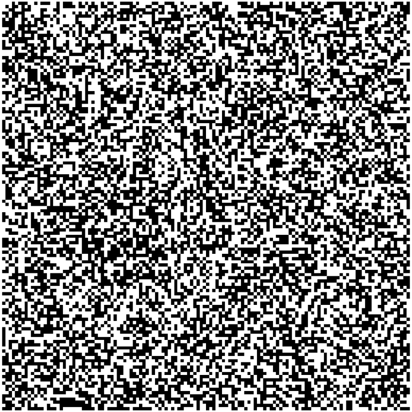
$$\sum_{1 \le d \le D} \max_{\substack{y,z \ge 0 \\ z-y \le x}} \max_{0 \le a < d} \left| \sum_{\substack{y \le n < z \\ n \equiv a \bmod d}} (-1)^{s(n)} \right| \le C x^{1-\eta}$$

for $D = x^{1-\varepsilon}$.

- This is a statement on *very short arithmetic progressions*: the Thue–Morse sequence usually shows cancellation along N-term arithmetic progressions having common difference $\sim N^R$, where $R > 0$ is arbitrary ($R \le 1.454$ for Fouvry–Mauduit).

Patterns in $\mathbf{t}$

$\mathbf{t}$ along short arithmetic subsequences even seems to behave randomly.

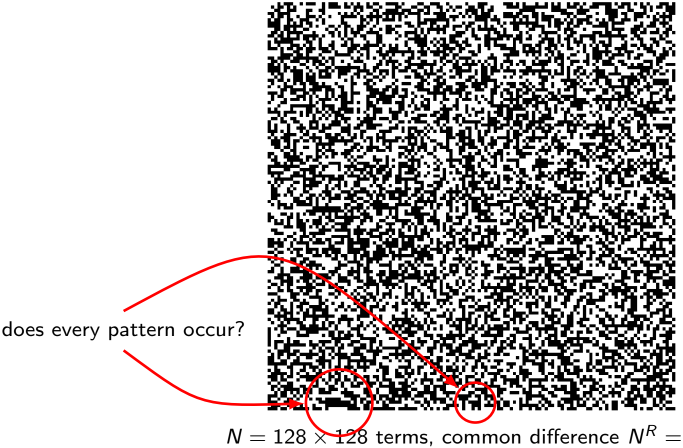


$N = 128 \times 128$ terms, common difference $N^R = 3^{21}$

We know that every finite sequence on $\{0, 1\}$ appears as an arithmetic subsequence of $\mathbf{t}$. But how often? ☕

Patterns in $\mathbf{t}$

$\mathbf{t}$ along short arithmetic subsequences even seems to behave randomly.



$N = 128 \times 128$ terms, common difference $N^R = 3^{21}$

We know that every finite sequence on $\{0, 1\}$ appears as an arithmetic subsequence of $\mathbf{t}$. But how often? ☕

Sparse infinite subsequences

We are interested in *Piatetski-Shapiro subsequences* of $\mathbf{t}$: for $c > 1$ not an integer we consider $\mathbf{t}(\lfloor n^c \rfloor)$.
For $1 < c < 2$ we can approximate $\lfloor n^c \rfloor$ by *Beatty sequences* $\lfloor n\alpha + \beta \rfloor$, and by the same method as for APs we can also prove a Beatty sequence variant of the level of distribution.

Corollary (S.)

Assume that $1 < c < 2$. Then the sequence $\mathbf{t}$ along $\lfloor n^c \rfloor$ attains both values 0 and 1 with asymptotic frequency $1/2$.

This improves Mauduit–Rivat 1995, 2005; S. 2014; Müllner–S. 2015.

- We also wish to obtain *normality* of Piatetski-Shapiro subsequences of $\mathbf{t}$! Every finite sequence in $\{0, 1\}^L$ should appear with asymptotic frequency 2^{-L} in the sequence $n \mapsto \mathbf{t}(\lfloor n^c \rfloor)$ for $1 < c < 2$, improving the range $1 < c < 3/2$ by Müllner and S. (2015).

Sparse infinite subsequences

We are interested in *Piatetski-Shapiro subsequences* of $\mathbf{t}$: for $c > 1$ not an integer we consider $\mathbf{t}(\lfloor n^c \rfloor)$.
For $1 < c < 2$ we can approximate $\lfloor n^c \rfloor$ by *Beatty sequences* $\lfloor n\alpha + \beta \rfloor$, and by the same method as for APs we can also prove a Beatty sequence variant of the level of distribution.

Corollary (S.)

Assume that $1 < c < 2$*. Then the sequence* $\mathbf{t}$ *along* $\lfloor n^c \rfloor$ *attains both values* 0 *and* 1 *with asymptotic frequency* $1/2$*.*

This improves Mauduit–Rivat 1995, 2005; S. 2014; Müllner–S. 2015.

- We also wish to obtain *normality* of Piatetski-Shapiro subsequences of $\mathbf{t}$! Every finite sequence in $\{0,1\}^L$ should appear with asymptotic frequency 2^{-L} in the sequence $n \mapsto \mathbf{t}(\lfloor n^c \rfloor)$ for $1 < c < 2$, improving the range $1 < c < 3/2$ by Müllner and S. (2015). ☕

Idea of proof of the level of distribution-result, I

In order to handle $\sum_{0\le n<x} \mathrm{e}(\vartheta s(nd+a))$, we successively reduce the digits to be taken into account by s. For an integer $\mu \ge 0$ we define the *truncation*

$$s_\mu(n) = s(n \bmod 2^\mu),$$

which is 2^μ-periodic.

The essential tool is *Van der Corput's inequality*.

Lemma

Let J be a finite interval containing N integers and let a_n be a complex number for $n \in J$. For all integers $R \ge 1$ we have

$$\left|\sum_{n\in J} a_n\right|^2 \le \frac{N+R-1}{R} \sum_{|r|<R} \left(1-\frac{|r|}{R}\right) \sum_{\substack{n\in J\\ n+r\in J}} a_{n+r}\overline{a_n}.$$

We only need to estimate *correlations*, where r is much smaller than n.

Idea of proof of the level of distribution-result, I

In order to handle $\sum_{0\le n<x}\mathrm{e}(\vartheta s(nd+a))$, we successively reduce the digits to be taken into account by s. For an integer $\mu\ge 0$ we define the *truncation*

$$s_\mu(n)=s(n \bmod 2^\mu),$$

which is 2^μ-periodic.

The essential tool is *Van der Corput's inequality*.

Lemma

Let J be a finite interval containing N integers and let a_n be a complex number for $n\in J$. For all integers $R\ge 1$ we have

$$\left|\sum_{n\in J}a_n\right|^2\le\frac{N+R-1}{R}\sum_{|r|<R}\left(1-\frac{|r|}{R}\right)\sum_{\substack{n\in J\\ n+r\in J}}a_{n+r}\overline{a_n}.$$

We only need to estimate *correlations*, where r is much smaller than n.

Idea of proof of the level of distribution-result, II

- Therefore the expression $\mathrm{e}(\vartheta s(nd + rd + a) - \vartheta s(nd + a))$ arises.
- The summand *rd* usually does not change the digits at indices significantly larger than $\log_2(rd)$, therefore we may replace s by the truncated version s_λ.
- This is Mauduit–Rivat 2009, 2010. The new thing is that we can apply this iteratively by using a variant of Van der Corput. In each step, we eliminate the digits between $\lambda - (j+1)\mu$ and $\lambda - j\mu$, until only the 2^τ-periodic function s_τ is left, where $\tau = \lambda - m\mu$.
- Since 2^τ is now much smaller than x, we have in fact reduced the problem to *long arithmetic progressions*: as n runs through $[0, x)$, the value nd is uniformly distributed in $\mathbb{Z}/2^\tau\mathbb{Z}$.
- Finally, we need an estimate of a so-called *Gowers uniformity norm* of the Thue–Morse sequence. This was found by Konieczny. □

Idea of proof of the level of distribution-result, II

- Therefore the expression $\mathrm{e}(\vartheta s(nd + rd + a) - \vartheta s(nd + a))$ arises.
- The summand rd usually does not change the digits at indices significantly larger than $\log_2(rd)$, therefore we may replace s by the truncated version s_λ.
- This is Mauduit–Rivat 2009, 2010. The new thing is that we can apply this iteratively by using a variant of Van der Corput. In each step, we eliminate the digits between $\lambda - (j+1)\mu$ and $\lambda - j\mu$, until only the 2^τ-periodic function s_τ is left, where $\tau = \lambda - m\mu$.
- Since 2^τ is now much smaller than x, we have in fact reduced the problem to *long arithmetic progressions*: as n runs through $[0, x)$, the value nd is uniformly distributed in $\mathbb{Z}/2^\tau\mathbb{Z}$.
- Finally, we need an estimate of a so-called *Gowers uniformity norm* of the Thue–Morse sequence. This was found by Konieczny. ☐

Idea of proof of the level of distribution-result, II

- Therefore the expression $\mathrm{e}(\vartheta s(nd + rd + a) - \vartheta s(nd + a))$ arises.
- The summand rd usually does not change the digits at indices significantly larger than $\log_2(rd)$, therefore we may replace s by the truncated version s_λ.
- This is Mauduit–Rivat 2009, 2010. The new thing is that we can apply this iteratively by using a variant of Van der Corput. In each step, we eliminate the digits between $\lambda - (j+1)\mu$ and $\lambda - j\mu$, until only the 2^τ-periodic function s_τ is left, where $\tau = \lambda - m\mu$.
- Since 2^τ is now much smaller than x, we have in fact reduced the problem to *long arithmetic progressions*: as n runs through $[0, x)$, the value nd is uniformly distributed in $\mathbb{Z}/2^\tau\mathbb{Z}$.
- Finally, we need an estimate of a so-called *Gowers uniformity norm* of the Thue–Morse sequence. This was found by Konieczny. □

Idea of proof of the level of distribution-result, II

- Therefore the expression $\mathrm{e}(\vartheta s(nd+rd+a)-\vartheta s(nd+a))$ arises.
- The summand rd usually does not change the digits at indices significantly larger than $\log_2(rd)$, therefore we may replace s by the truncated version s_λ.
- This is Mauduit–Rivat 2009, 2010. The new thing is that we can apply this iteratively by using a variant of Van der Corput. In each step, we eliminate the digits between $\lambda-(j+1)\mu$ and $\lambda-j\mu$, until only the 2^τ-periodic function s_τ is left, where $\tau=\lambda-m\mu$.
- Since 2^τ is now much smaller than x, we have in fact reduced the problem to *long arithmetic progressions*: as n runs through $[0,x)$, the value nd is uniformly distributed in $\mathbb{Z}/2^\tau\mathbb{Z}$.
- Finally, we need an estimate of a so-called *Gowers uniformity norm* of the Thue–Morse sequence. This was found by Konieczny. □

The level of distribution of Zeckendorf

Let $Z(n)$ be the *Zeckendorf sum of digits* of n, that is, the minimal number of Fibonacci numbers needed to write n as their sum. The following result will be ready soon. ☕

Theorem (Drmota, Müllner, S., in preparation)

The Zeckendorf sum-of-digits function modulo 2 *has level of distribution* 1*. More precisely, for all* $\varepsilon > 0$ *we have*

$$\sum_{1\le d\le D} \max_{\substack{y,z\ge 0\\ z-y\le x}} \max_{0\le a<d} \left| \sum_{\substack{y\le n<z\\ n\equiv a \bmod d}} (-1)^{Z(n)} \right| = \mathcal{O}(x^{1-\eta})$$

for some $\eta > 0$ *depending on* ε*, where* $D = x^{1-\varepsilon}$.

Cutting away Zeckendorf digits

- To handle the sum $\sum_{0\le n<N} \mathrm{e}(\vartheta Z(nd+a))$, we proceed as in the Thue–Morse case.
- We first cut away the digits at indices $\geq \lambda$: for $\lambda \geq 2$ define the truncation v_k (which is not periodic!) by

$$v_k(\varepsilon_2 F_2 + \varepsilon_3 F_3 + \cdots) = \varepsilon_2 F_2 + \cdots + \varepsilon_{\lambda-1} F_{\lambda-1},$$

  and set $Z_\lambda(n) = Z(v_\lambda(n))$.
- Next, we cut away digits with indices in $\bigl[\lambda-(j+1)\mu, \lambda-j\mu\bigr)$. This can be accomplished (again) by a variant of Van der Corput's inequality.
- We are left with the function Z_τ, where $\tau = \lambda - m\mu$; the digits below τ of $nd+a$ assume every combination the expected number of times. Therefore we can replace the sum over $nd+a$ by a full sum over n!
- We also need to detect the Zeckendorf digits with indices in $J=[a,b)$ in an analytical way.

Cutting away Zeckendorf digits

- To handle the sum $\sum_{0\le n<N} \mathrm{e}(\vartheta Z(nd+a))$, we proceed as in the Thue–Morse case.
- We first cut away the digits at indices $\geq \lambda$: for $\lambda \geq 2$ define the truncation v_k (which is not periodic!) by

$$v_k(\varepsilon_2 F_2 + \varepsilon_3 F_3 + \cdots) = \varepsilon_2 F_2 + \cdots + \varepsilon_{\lambda-1} F_{\lambda-1},$$

  and set $Z_\lambda(n) = Z(v_\lambda(n))$.
- Next, we cut away digits with indices in $\bigl[\lambda-(j+1)\mu, \lambda-j\mu\bigr)$. This can be accomplished (again) by a variant of Van der Corput's inequality.
- We are left with the function Z_τ, where $\tau = \lambda - m\mu$; the digits below τ of $nd+a$ assume every combination the expected number of times. Therefore we can replace the sum over $nd+a$ by a full sum over n!
- We also need to detect the Zeckendorf digits with indices in $J = [a, b)$ in an analytical way.

Cutting away Zeckendorf digits

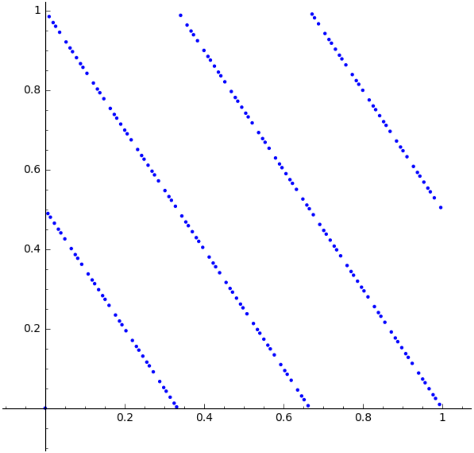
- To handle the sum $\sum_{0\le n<N} \mathrm{e}(\vartheta Z(nd+a))$, we proceed as in the Thue–Morse case.
- We first cut away the digits at indices $\ge \lambda$: for $\lambda \ge 2$ define the truncation v_k (which is not periodic!) by

  $$v_k(\varepsilon_2 F_2 + \varepsilon_3 F_3 + \cdots) = \varepsilon_2 F_2 + \cdots + \varepsilon_{\lambda-1} F_{\lambda-1},$$

  and set $Z_\lambda(n) = Z(v_\lambda(n))$.
- Next, we cut away digits with indices in $\bigl[\lambda-(j+1)\mu, \lambda-j\mu\bigr)$. This can be accomplished (again) by a variant of Van der Corput's inequality.
- We are left with the function Z_τ, where $\tau = \lambda - m\mu$; the digits below τ of $nd+a$ assume every combination the expected number of times. Therefore we can replace the sum over $nd+a$ by a full sum over n!
- We also need to detect the Zeckendorf digits with indices in $J=[a,b)$ in an analytical way.

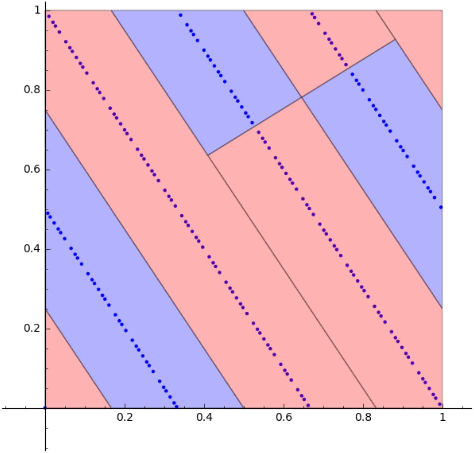
Two-dimensional detection

We introduce the function $p : \mathbb{N} \to \mathbb{R}^2$ by $p_k(n) = \left(\frac{n}{\varphi^k}, \frac{n}{\varphi^{k+1}}\right)$. The closure of the set of points $p_k(n)$ mod $(1, 1)$ is a finite set of lines with slope $-F_{k+1}/F_k$. Example for $k = 3$: slope $-3/2$.



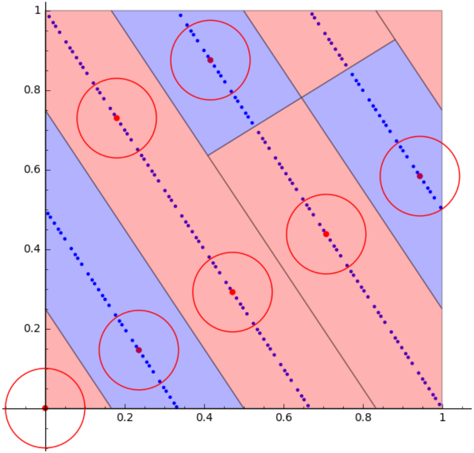
Two-dimensional detection

We introduce the function $p : \mathbb{N} \to \mathbb{R}^2$ by $p_k(n) = \left(\frac{n}{\varphi^k}, \frac{n}{\varphi^{k+1}}\right)$. The closure of the set of points $p_k(n)$ mod $(1, 1)$ is a finite set of lines with slope $-F_{k+1}/F_k$. Example for $k = 3$: slope $-3/2$.



Two-dimensional detection

We introduce the function $p : \mathbb{N} \to \mathbb{R}^2$ by $p_k(n) = \left(\frac{n}{\varphi^k}, \frac{n}{\varphi^{k+1}}\right)$. The closure of the set of points $p_k(n)$ mod $(1, 1)$ is a finite set of lines with slope $-F_{k+1}/F_k$. Example for $k = 3$: slope $-3/2$.



0
1
10
100
101
1000
1001

Two-dimensional detection of digits

We define parallelograms A_k and B_k:

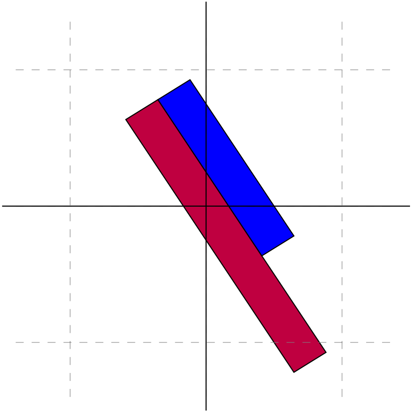
$$\begin{array}{c|c} A_k & B_k \\ -\frac{1}{2} \le F_{k+1}x + F_k y < \frac{1}{2} & -\frac{1}{2} \le F_{k+1}x + F_k y < \frac{1}{2} \\ -\varphi \le -\frac{1}{\varphi}x + y < 1 & -\frac{1}{\varphi} \le -\frac{1}{\varphi}x + y < 1. \end{array}$$

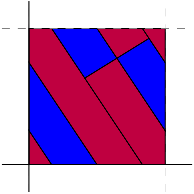
With their help we define shifted parallelograms R_u:

$$R_k(u) = p_k(u) + \begin{cases} A_k, & 0 \le u < F_{k-1} \\ B_k, & F_{k-1} \le u < F_k. \end{cases}$$

The sets $R_k(u) + \mathbb{Z}^2$ form a partition of $\mathbb{R}^2$ and we have $v_k(n) = u$ if and only if $p_k(n) \in R_k(u) + \mathbb{Z}^2$.

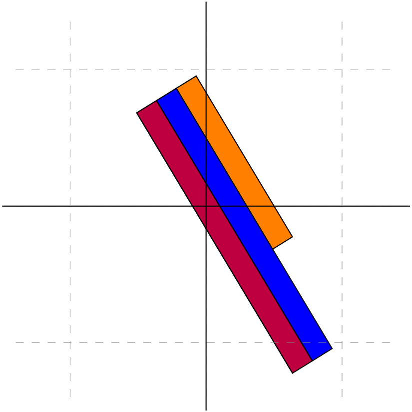
The regions R_u: 1 significant digit

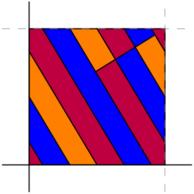




$0, 1$

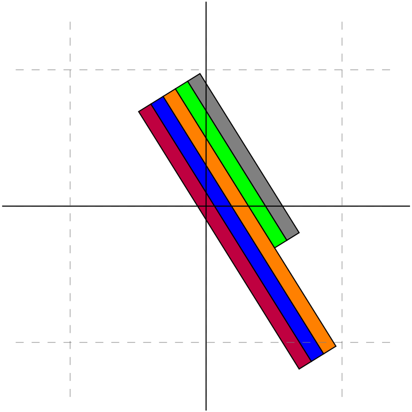
The regions R_u: 2 significant digits

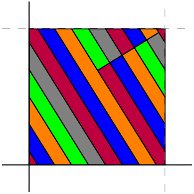




$00, 01, 10$

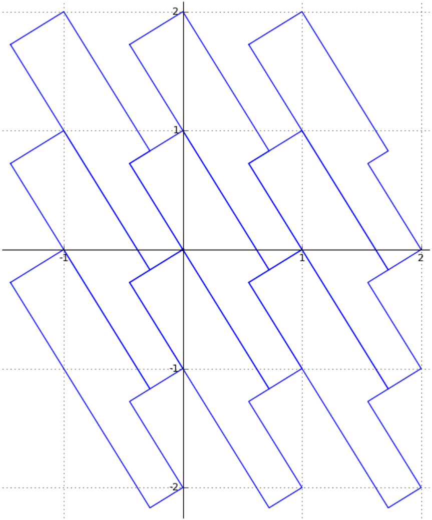
The regions R_u: 3 significant digits





$000, 001, 010, 100, 101$

The limiting fundamental domain



Finishing the proof idea

- Applying Fourier approximation of suitable regions, we obtain an analytic expression that is close to 1 if the Zeckendorf digits in $J = [a, b)$ are equal to prescribed values, and close to 0 otherwise.
- Finally, we need a *Gowers uniformity norm* of the Zeckendorf sum-of-digits function. These norms are certain iterated correlations and arise from the repeated application of Van der Corput-type inequalities: we need to estimate

$$\sum_{0\le n,h_1,\ldots,h_r<F_\lambda} \prod_{\varepsilon_1,\ldots,\varepsilon_r\in\{0,1\}} \mathrm{e}\bigl(\vartheta(-1)^{\varepsilon_1+\cdots+\varepsilon_r} Z_\lambda(n+\varepsilon_1 h_1+\cdots+\varepsilon_r h_r)\bigr).$$

This was contributed by Müllner. ☐

Current work: prime numbers

- We want to prove a *prime number theorem* for the Zeckendorf sum-of-digits function: asymptotically one half of the prime numbers should have an even Zeckendorf sum of digits.
- This extends a theorem by Mauduit and Rivat on the base-q sum of digits of prime numbers.
- It is sufficient to treat *sums of type I and II*:

$$S_{\mathrm{I}} = \sum_{m} \max_{I} \left| \sum_{n \in I} (-1)^{Z(mn)} \right|;$$

$$S_{\mathrm{II}} = \sum_{m} \sum_{n} a_m b_n (-1)^{Z(mn)}.$$

- Our level of distribution-result allows us to choose m very large and n very small in S_{I}; this reduces the amount of work necessary for S_{II}!

Medium-term goals, part II

- Prove a prime number theorem for the Zeckendorf sum-of-digits function.
- Prove the following: for all k large enough there exists a prime number that is the sum of k different Fibonacci numbers ($\rightarrow$ jointly with Drmota and Müllner).
- Normality of $\mathbf{t}$ and $Z(n)$ mod 2 along $\lfloor n^c \rfloor$ for $1 < c < 2$.

Thank you![1]

---

[1] Supported by the ANR-FWF project MuDeRa, and by the FWF, Project F55.