The digits of $n + t$

Lukas Spiegelhofer[1]

December 15, 2020, One World Numeration Seminar

[1]This talk is about joint work with Michael Wallner (TU Wien)

The fundamental question

We write n in base 2:

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

where $\varepsilon_j \in \{0, 1\}$. The vector $(\varepsilon_j)_{j \geq 0}$ is the *binary expansion* of n.

What happens to the binary expansion of n when a constant t is added?

Complementary to Sakarovitch's talk four weeks ago:

Adding 1 in general numeration systems vs. Adding t in base 2

The fundamental question

We write n in base 2:

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

where $\varepsilon_j \in \{0, 1\}$. The vector $(\varepsilon_j)_{j \geq 0}$ is the *binary expansion* of n.

> *What happens to the binary expansion of n when a constant t is added?*

Complementary to Sakarovitch's talk four weeks ago:

Adding 1 in general numeration systems vs. Adding t in base 2

The fundamental question

We write n in base 2:

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

where $\varepsilon_j \in \{0, 1\}$. The vector $(\varepsilon_j)_{j \geq 0}$ is the *binary expansion* of n.

> *What happens to the binary expansion of n when a constant t is added?*

Complementary to Sakarovitch's talk four weeks ago:

Adding 1 in general numeration systems   vs.   Adding t in base 2

Addition of 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.

$$*\,011\cdots1 \mapsto *100\cdots0 \tag{1}$$

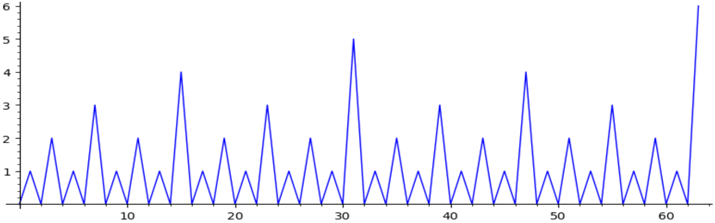
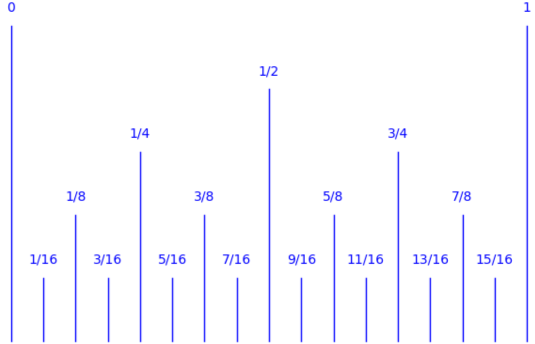


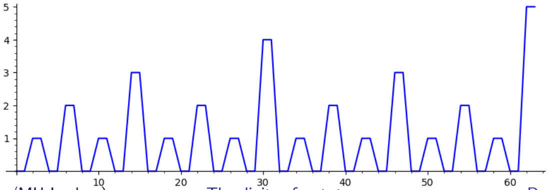
Figure: The number of carries in the addition $n+1$

This is the *ruler sequence* $n \mapsto \nu_2(n+1)$, given by the exponent of two in the prime factorization of $n+1$.

The following picture is well known in countries using imperial units.



$t = 2$ is similar: ε_0 is unchanged and (1) is applied for the remaining digits.



The case $t \geq 3$

The fun begins. For $t = 3$ we have the following cases:

$$*00 \mapsto *11; \qquad *01^k01 \mapsto *10^k00;$$
$$*01^k10 \mapsto *10^k01; \qquad *01^k11 \mapsto *10^k10.$$

- Of course, we can find such a case distinction for each t in a straightforward way. This describes the situation for any given t completely.
- However: for growing t, we obtain long case distinctions. A structural principle describing these cases is unavailable.
- This is of course due to *carry propagation*. Carries can propagate through many blocks of 1, and many cases occur.

$$\begin{array}{rr} & 11101001110110011 \\ + & 10110001001101 \end{array}$$

The case $t \geq 3$

The fun begins. For $t = 3$ we have the following cases:

$$*00 \mapsto *11; \qquad *01^k01 \mapsto *10^k00;$$
$$*01^k10 \mapsto *10^k01; \qquad *01^k11 \mapsto *10^k10.$$

- Of course, we can find such a case distinction for each t in a straightforward way. This describes the situation for any given t completely.
- However: for growing t, we obtain long case distinctions. A structural principle describing these cases is unavailable.
- This is of course due to *carry propagation*. Carries can propagate through many blocks of 1, and many cases occur.

$$\begin{array}{r} 11101001110110011 \\ + \quad 10110001001101 \end{array}$$

The case $t \geq 3$

The fun begins. For $t = 3$ we have the following cases:

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

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

- Of course, we can find such a case distinction for each t in a straightforward way. This describes the situation for any given t completely.
- However: for growing t, we obtain long case distinctions. A structural principle describing these cases is unavailable.
- This is of course due to *carry propagation*. Carries can propagate through many blocks of 1, and many cases occur.

$$\begin{array}{rr} & 11101001110110011 \\ + & 10110001001101 \end{array}$$

The case $t \geq 3$

The fun begins. For $t = 3$ we have the following cases:

$$*00 \mapsto *11; \qquad *01^k01 \mapsto *10^k00;$$
$$*01^k10 \mapsto *10^k01; \qquad *01^k11 \mapsto *10^k10.$$

- Of course, we can find such a case distinction for each t in a straightforward way. This describes the situation for any given t completely.
- However: for growing t, we obtain long case distinctions. A structural principle describing these cases is unavailable.
- This is of course due to *carry propagation*. Carries can propagate through many blocks of 1, and many cases occur.

$$\begin{array}{r} 111010011101110011 \\ + \quad 10110001001101 \end{array}$$

An observation

We do not fully understand addition in base 2.

It is difficult enough to consider the sum-of-digits function $s_2(n)$. We have the formula (Legendre)

$$s_2(n+t) = s_2(n) + s_2(t) - \nu_2\left(\binom{n+t}{t}\right).$$

The function s_2 can be used to count the number of carries in $n+t$: a well-known relation due to Kummer is

$$\nu_2\left(\binom{n+t}{t}\right) = \#\mathrm{carries}(n,t).$$

We forget the carry *structure* and only keep the *number* of carries.

An observation

We do not fully understand addition in base 2.

It is difficult enough to consider the sum-of-digits function $s_2(n)$. We have the formula (Legendre)

$$s_2(n+t) = s_2(n) + s_2(t) - \nu_2\left(\binom{n+t}{t}\right).$$

The function s_2 can be used to count the number of carries in $n+t$: a well-known relation due to Kummer is

$$\nu_2\left(\binom{n+t}{t}\right) = \#\mathrm{carries}(n,t).$$

We forget the carry *structure* and only keep the *number* of carries.

An observation

We do not fully understand addition in base 2.

It is difficult enough to consider the sum-of-digits function $s_2(n)$. We have the formula (Legendre)

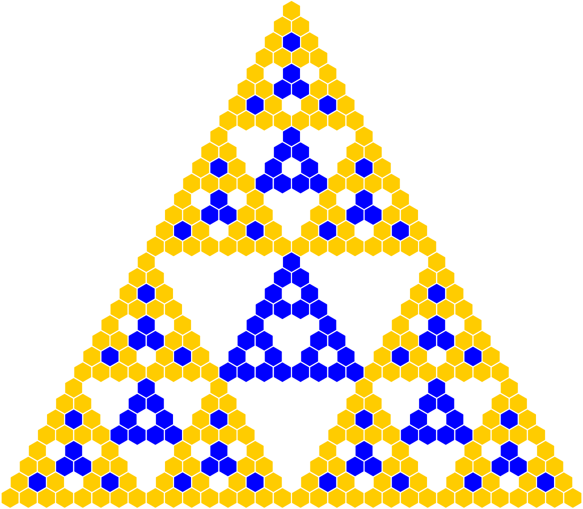
$$s_2(n+t) = s_2(n) + s_2(t) - \nu_2\left(\binom{n+t}{t}\right).$$

The function s_2 can be used to count the number of carries in $n+t$: a well-known relation due to Kummer is

$$\nu_2\left(\binom{n+t}{t}\right) = \#\mathrm{carries}(n,t).$$

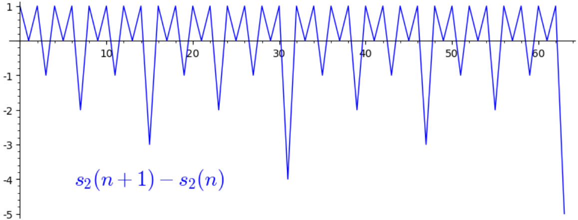
We forget the carry *structure* and only keep the *number* of carries.

The 2-valuation of binomial coefficients

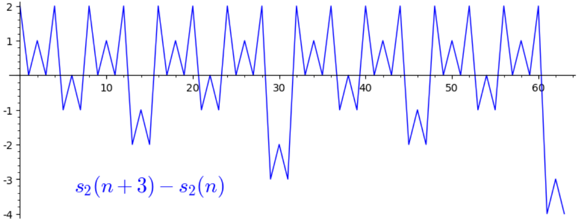


Two examples

We have $s_2(n+1) - s_2(n) = 1 - \nu_2\big(n+1\big)$:



Summing three consecutive values, we obtain the case $t = 3$.



What proportion of the graph is above the x-axis?

An apparently simple, unsolved conjecture is due to T. W. Cusick. Let $t \geq 0$ be an integer.

Is it true that, more often than not, we have $s_2(n+t) \geq s_2(n)$?

In symbols, we seek to prove $c_t > 1/2$, where

$$c_t = \lim_{N \to \infty} \frac{1}{N} \bigl| \{ 0 \leq n < N : s_2(n+t) \geq s_2(n) \} \bigr|.$$

For example,

$$c_1 = 3/4, \quad c_{21} = 5/8, \quad c_{999} = 37561/2^{16},$$

$$\min_{t \leq 2^{30}} c_t = 18169025645289/2^{45} = 0.516\ldots.$$

The latter minimum is attained at

$$t = (111101111011110111101111011111)_2 \text{ and}$$

$$t^R = (111110111101111011110111101111)_2.$$

What proportion of the graph is above the x-axis?

An apparently simple, unsolved conjecture is due to T. W. Cusick. Let $t \geq 0$ be an integer.

Is it true that, more often than not, we have $s_2(n+t) \geq s_2(n)$?

In symbols, we seek to prove $c_t > 1/2$, where

$$c_t = \lim_{N \to \infty} \frac{1}{N} \left| \{ 0 \leq n < N : s_2(n+t) \geq s_2(n) \} \right|.$$

For example,

$$c_1 = 3/4, \quad c_{21} = 5/8, \quad c_{999} = 37561/2^{16},$$
$$\min_{t \leq 2^{30}} c_t = 18169025645289/2^{45} = 0.516\ldots.$$

The latter minimum is attained at

$$t = (111101111011110111101111011111)_2 \text{ and}$$
$$t^R = (111110111101111011110111101111)_2.$$

Densities for Cusick's conjecture

More generally, for integers $t \geq 0$ and j we define

$$\delta(j,t) = \lim_{N\to\infty} \frac{1}{N} \bigl| \{0 \leq n < N : s_2(n+t) - s_2(n) = j\} \bigr|.$$

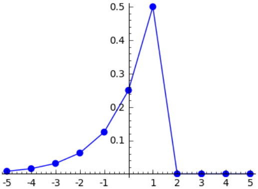
- The densities $\delta(j,t)$ give us a probability distribution on $\mathbb{Z}$ for each t.

Densities for Cusick's conjecture

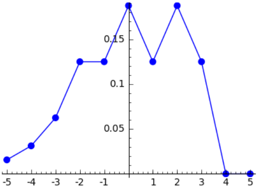
More generally, for integers $t \geq 0$ and j we define

$$\delta(j,t) = \lim_{N\to\infty} \frac{1}{N} \left| \{0 \leq n < N : s_2(n+t) - s_2(n) = j\} \right|.$$

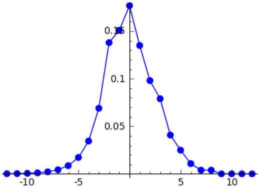
- The densities $\delta(j,t)$ give us a probability distribution on $\mathbb{Z}$ for each t.



$t = 1$



$t = 21$



$t = 999$

A two-dimensional recurrence

The array δ satisfies the recurrence

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

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

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

This permits to compute $\delta(j,t)$ efficiently. In particular, $c_t > 1/2$ for $t \leq 2^{30}$. ($\approx$ 2 CPU hours, using a C program)

The first theorem

Let $M = M(t)$ be the number of blocks of 1s in the binary expansion of t.

Theorem (S.–Wallner 2020+)

Set $A_2(1) = 1$, *and for* $t \geq 1$ *let* $A_2(2t) = A_2(t)$, *and*

$$A_2(2t+1) = \frac{A_2(t) + A_2(t+1) + 1}{2}.$$

If M *is larger than some absolute, effective constant* M_0, *we have*

$$\delta(j,t) = \frac{1}{\sqrt{4\pi A_2(t)}} \exp\left(-\frac{j^2}{4A_2(t)}\right) + \mathcal{O}\left(\frac{(\log M)^4}{M}\right)$$

for all integers j. *The implied constant is absolute.*

This improves on a theorem by Emme and Hubert (2018).

A corollary

The number M of blocks of 1s in t satisfies $M \asymp A_2(t)$, the width of the normal distribution is therefore $\asymp \sqrt{M}$. We obtain the following result.

Corollary

There exists an absolute constant $C > 0$ with the following property. For all $t \geq 1$ we have

$$c_t \geq 1/2 - C\bigl(\log M\bigr)^5 M^{-1/2},$$

where M is the number of blocks of 1s in t.

The second theorem

Again, let $M = M(t)$ be the number of blocks of 1s in t.

Theorem (S.–Wallner 2020+)

Let $t \geq 1$. If $M(t)$ is larger than some absolute, effective constant M_1, then $c_t > 1/2$.

Cusick: "Your paper reduces my conjecture to what I will call the 'hard cases' [...]". $\longrightarrow$ more work to do!

The second theorem

Again, let $M = M(t)$ be the number of blocks of 1s in t.

Theorem (S.–Wallner 2020+)

Let $t \geq 1$. If $M(t)$ is larger than some absolute, effective constant M_1, then $c_t > 1/2$.

Cusick: "Your paper reduces my conjecture to what I will call the 'hard cases' [...]". $\longrightarrow$ more work to do!

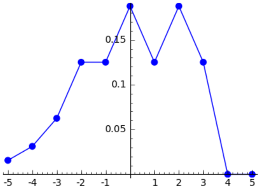
The second theorem

Again, let $M = M(t)$ be the number of blocks of 1s in t.

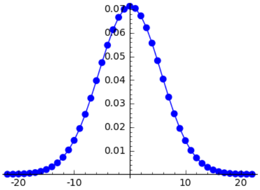
Theorem (S.–Wallner 2020+)

Let $t \geq 1$. If $M(t)$ is larger than some absolute, effective constant M_1, then $c_t > 1/2$.

Cusick: "Your paper reduces my conjecture to what I will call the 'hard cases' [...]". $\longrightarrow$ more work to do!



hard



easier

Method of proof of the theorems

Consider the characteristic function (writing $\mathrm{e}(x) = \exp(2\pi i x)$)

$$\gamma_t(\vartheta) = \lim_{N\to\infty} \frac{1}{N} \sum_{0\le n<N} \mathrm{e}\bigl(\vartheta s_2(n+t) - \vartheta s_2(n)\bigr) = \sum_{j\in\mathbb{Z}} \delta(j,t)\,\mathrm{e}(j\vartheta).$$

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

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

Note that $\gamma_t(0) = 1$; it follows that $\operatorname{Re}\gamma_t(x) > 0$ in a disk $D_t(0)$, and we can consider $\log\gamma_t(x)$ on D_t ($\longrightarrow$ "*cumulant generating function*".)

Method of proof of the theorems

Consider the characteristic function (writing $\mathrm{e}(x) = \exp(2\pi i x)$)

$$\gamma_t(\vartheta) = \lim_{N\to\infty} \frac{1}{N} \sum_{0\le n<N} \mathrm{e}\bigl(\vartheta s_2(n+t) - \vartheta s_2(n)\bigr) = \sum_{j\in\mathbb{Z}} \delta(j,t)\,\mathrm{e}(j\vartheta).$$

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

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

Note that $\gamma_t(0) = 1$; it follows that $\mathrm{Re}\,\gamma_t(x) > 0$ in a disk $D_t(0)$, and we can consider $\log\gamma_t(x)$ on D_t ($\longrightarrow$ "*cumulant generating function*".)

Method of proof of the theorems

We have $\gamma_t(\vartheta) = 1 + \mathcal{O}(\vartheta^2)$, therefore

$$\gamma_t(\vartheta) = \exp\left(-\sum_{j\geq 2} A_j(t)(2\pi\vartheta)^j\right)$$

for some $A_j(t) \in \mathbb{C}$ and all $\vartheta \in D_t$.

- Up to multiplication by i^j, the values $A_j(t)$ are the *cumulants* of $\delta(\cdot, t)$.
- We abbreviate $a_j = A_j(t)$, $b_j = A_j(t+1)$, $c_j = A_j(2t+1)$. The recurrence for γ_t gives

$$\begin{aligned}\exp\bigl(-c_2\vartheta^2 - c_3\vartheta^3 - \cdots\bigr) &= \tfrac{1}{2}\exp\bigl(\quad i\,\vartheta - a_2\vartheta^2 - a_3\vartheta^3 - \cdots\bigr)\\ &\quad + \tfrac{1}{2}\exp\bigl(-i\,\vartheta - b_2\vartheta^2 - b_3\vartheta^3 - \cdots\bigr),\end{aligned}$$

valid for ϑ in a certain disk.

Method of proof of the theorems

We have $\gamma_t(\vartheta) = 1 + \mathcal{O}(\vartheta^2)$, therefore

$$\gamma_t(\vartheta) = \exp\left(-\sum_{j\geq 2} A_j(t)(2\pi\vartheta)^j\right)$$

for some $A_j(t) \in \mathbb{C}$ and all $\vartheta \in D_t$.

- Up to multiplication by i^j, the values $A_j(t)$ are the *cumulants* of $\delta(\cdot, t)$.
- We abbreviate $a_j = A_j(t)$, $b_j = A_j(t+1)$, $c_j = A_j(2t+1)$. The recurrence for γ_t gives

$$\begin{aligned}\exp\bigl(-c_2\vartheta^2 - c_3\vartheta^3 - \cdots\bigr) &= \tfrac{1}{2}\exp\bigl(\quad i\,\vartheta - a_2\vartheta^2 - a_3\vartheta^3 - \cdots\bigr)\\ &\quad + \tfrac{1}{2}\exp\bigl(-i\,\vartheta - b_2\vartheta^2 - b_3\vartheta^3 - \cdots\bigr),\end{aligned}$$

valid for ϑ in a certain disk.

Comparing coefficients

We obtain a recurrence for the cumulants:

$$
\begin{aligned}
c_2 &= \frac{a_2+b_2}{2} + \frac{1}{2};\\
c_3 &= \frac{a_3+b_3}{2} + i\frac{a_2-b_2}{2};\\
c_4 &= \frac{a_4+b_4}{2} + i\frac{a_3-b_3}{2} - \frac{(a_2-b_2)^2}{8} + \frac{1}{12};\\
c_5 &= \frac{a_5+b_5}{2} + i\frac{a_4-b_4}{2} - \frac{(a_2-b_2)(a_3-b_3)}{4} + i\frac{a_2-b_2}{6}.
\end{aligned}
$$

For the normal distribution result, we only have to consider A_2; for Cusick's conjecture, we also have to take A_3, A_4, A_5 into account. This precision is necessary since the case $c_t \le 1/2 + M^{-3/2}$ can occur!

Comparing coefficients

We obtain a recurrence for the cumulants:

$$\begin{aligned}
c_2 &= \frac{a_2+b_2}{2}+\frac{1}{2};\\
c_3 &= \frac{a_3+b_3}{2}+i\frac{a_2-b_2}{2};\\
c_4 &= \frac{a_4+b_4}{2}+i\frac{a_3-b_3}{2}-\frac{(a_2-b_2)^2}{8}+\frac{1}{12};\\
c_5 &= \frac{a_5+b_5}{2}+i\frac{a_4-b_4}{2}-\frac{(a_2-b_2)(a_3-b_3)}{4}+i\frac{a_2-b_2}{6}.
\end{aligned}$$

For the normal distribution result, we only have to consider A_2; for Cusick's conjecture, we also have to take A_3, A_4, A_5 into account. This precision is necessary since the case $c_t \le 1/2 + M^{-3/2}$ can occur!

Proof of the first theorem, I

We define the approximation

$$\gamma'_t(\vartheta) = \exp\bigl(-A_2(t)(2\pi\vartheta)^2\bigr)$$

as well as the error

$$\widetilde{\gamma}_t(\vartheta) = \gamma_t(\vartheta) - \gamma'_t(\vartheta).$$

Proposition

There exists an absolute constant C such that for all t having M blocks of 1s and $|\vartheta| \le \min\bigl(M^{-1/3}, 1/(4\pi)\bigr)$ we have

$$\bigl|\widetilde{\gamma}_t(\vartheta)\bigr| \le CM\vartheta^3.$$

Proposition

Assume that $t \ge 1$ has at least M blocks of 1s. Then for $|\vartheta| \le 1/2$,

$$\bigl|\gamma_t(\vartheta)\bigr| \ll \exp\left(-\frac{M\vartheta^2}{4}\right).$$

Proof of the first theorem, I

We define the approximation

$$\gamma'_t(\vartheta) = \exp\bigl(-A_2(t)(2\pi\vartheta)^2\bigr)$$

as well as the error

$$\widetilde{\gamma}_t(\vartheta) = \gamma_t(\vartheta) - \gamma'_t(\vartheta).$$

Proposition

There exists an absolute constant C such that for all t having M blocks of 1s and $|\vartheta| \le \min\bigl(M^{-1/3}, 1/(4\pi)\bigr)$ we have

$$\bigl|\widetilde{\gamma}_t(\vartheta)\bigr| \le CM\vartheta^3.$$

Proposition

Assume that $t \ge 1$ has at least M blocks of 1s. Then for $|\vartheta| \le 1/2$,

$$\bigl|\gamma_t(\vartheta)\bigr| \ll \exp\left(-\frac{M\vartheta^2}{4}\right).$$

Proof of the first theorem, I

We define the approximation

$$\gamma'_t(\vartheta) = \exp\bigl(-A_2(t)(2\pi\vartheta)^2\bigr)$$

as well as the error

$$\widetilde{\gamma}_t(\vartheta) = \gamma_t(\vartheta) - \gamma'_t(\vartheta).$$

Proposition

There exists an absolute constant C such that for all t having M blocks of 1s and $|\vartheta| \le \min\bigl(M^{-1/3}, 1/(4\pi)\bigr)$ we have

$$\bigl|\widetilde{\gamma}_t(\vartheta)\bigr| \le CM\vartheta^3.$$

Proposition

Assume that $t \ge 1$ has at least M blocks of 1s. Then for $|\vartheta| \le 1/2$,

$$\bigl|\gamma_t(\vartheta)\bigr| \ll \exp\left(-\frac{M\vartheta^2}{4}\right).$$

Proof of the first theorem, II

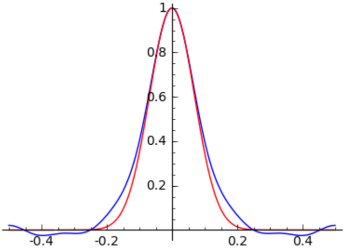


Figure: Illustrating the propositions for $t = 123$.

We combine these facts with the formula

$$\delta(j, t) = \int_{-1/2}^{1/2} \gamma_t(\vartheta)\, \mathrm{e}(-j\vartheta)\, \mathrm{d}\vartheta.$$

After extending to a complete Gauss integral we obtain the statement of the theorem (with $\sqrt{\pi}$ and everything).

Recapturing the first theorem

Theorem (S.–Wallner 2020+)

Set $A_2(1) = 1$*, and for* $t \geq 1$ *let* $A_2(2t) = A_2(t)$*, and*

$$A_2(2t+1) = \frac{A_2(t) + A_2(t+1) + 1}{2}.$$

If M *is larger than some absolute, effective constant* M_0*, we have*

$$\delta(j,t) = \frac{1}{\sqrt{4\pi A_2(t)}} \exp\left(-\frac{j^2}{4A_2(t)}\right) + \mathcal{O}\left(\frac{(\log M)^4}{M}\right)$$

for all integers j*. The implied constant is absolute.*

Proof of the second theorem

For c_t we need a more precise asymptotic expansion, involving the cumulants $A_2(t), A_3(t), A_4(t)$, and $A_5(t)$ — we study a *distorted* normal distribution.
We use the approximation

$$\gamma'_t(\vartheta) = \exp\left(-\sum_{2\le j\le 5} A_j(t)(2\pi\vartheta)^j\right)$$

and the error

$$\widetilde{\gamma}_t(\vartheta) = \gamma_t(\vartheta) - \gamma'_t(\vartheta).$$

As above, we have

$$\left|\widetilde{\gamma}_t(\vartheta)\right| \le CM\vartheta^6 \text{ for } |\vartheta| \le \min\left(M^{-1/6}, 1/(4\pi)\right)$$

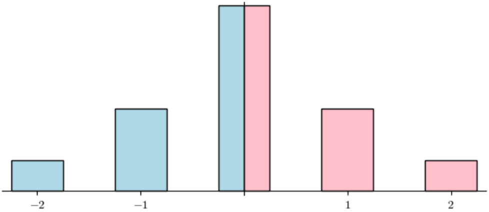
with an absolute constant C.

Reconstructing c_t

- The values $c_t = \delta(0,t) + \delta(1,t) + \cdots$ are related to the CF $\gamma_t(\vartheta)$ by the formula

$$c_t = \frac{1}{2} + \frac{\delta(0,t)}{2} + \frac{1}{2}\int_{-1/2}^{1/2} \operatorname{Im}\gamma_t(\vartheta)\cot(\pi\vartheta)\mathrm{d}\vartheta.$$

- Note that the third summand is zero if $\delta(-j,t) = \delta(j,t)$ for all j, and $c_t > 1/2$ follows in this case.

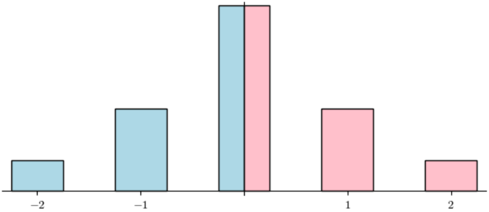


Reconstructing c_t

- The values $c_t = \delta(0,t) + \delta(1,t) + \cdots$ are related to the CF $\gamma_t(\vartheta)$ by the formula

$$c_t = \frac{1}{2} + \frac{\delta(0,t)}{2} + \frac{1}{2}\int_{-1/2}^{1/2} \operatorname{Im}\gamma_t(\vartheta)\cot(\pi\vartheta)\mathrm{d}\vartheta.$$

- Note that the third summand is zero if $\delta(-j,t) = \delta(j,t)$ for all j, and $c_t > 1/2$ follows in this case.



Reconstructing c_t

- In this identity, we will replace γ_t by γ_t'. We expand the exponential:

$$\gamma_t'(\vartheta) = \exp\bigl(-A_2(t)(\tau\vartheta)^2\bigr) \times \Bigl(1 - A_3(t)(\tau\vartheta)^3 - A_4(t)(\tau\vartheta)^4 - A_5(\tau\vartheta)^5 + \frac{1}{2}A_3(t)^2(\tau\vartheta)^6 + A_3(t)A_4(t)(\tau\vartheta)^7 - \frac{1}{6}A_3(t)^3(\tau\vartheta)^9\Bigr) + \mathcal{O}(E),$$

where $\tau = 2\pi$ and E is a certain error.

Reconstructing c_t

- Introducing complete Gauss integrals, this leads to an approximation of c_t:

$$c_t = \frac{1}{2} + \frac{1}{4\sqrt{\pi}} \left(A_2^{-1/2} + iA_2^{-3/2} A_3 + \frac{3}{4} A_2^{-5/2} \left(2i\, A_5 - A_4 - \frac{i\, A_3}{6} \right) + \frac{15}{8} A_2^{-7/2} \left(\frac{A_3}{2} - 2i\, A_4 \right) A_3 + \frac{35}{16} i\, A_2^{-9/2} A_3^3 \right) + \mathcal{O}(E).$$

- The red terms sometimes almost cancel. Therefore we need more cumulants!
- A closer look at the recurrences for A_j finishes the proof: for $c_t > 1/2$ it is sufficient to have many blocks of 1s in the binary expansion of t.

Reconstructing c_t

- Introducing complete Gauss integrals, this leads to an approximation of c_t:

$$c_t = \frac{1}{2} + \frac{1}{4\sqrt{\pi}} \left(A_2^{-1/2} + iA_2^{-3/2} A_3 + \frac{3}{4} A_2^{-5/2} \left(2i\, A_5 - A_4 - \frac{i\, A_3}{6} \right) + \frac{15}{8} A_2^{-7/2} \left(\frac{A_3}{2} - 2i\, A_4 \right) A_3 + \frac{35}{16} i\, A_2^{-9/2} A_3^3 \right) + \mathcal{O}(E).$$

- The red terms sometimes almost cancel. Therefore we need more cumulants!
- A closer look at the recurrences for A_j finishes the proof: for $c_t > 1/2$ it is sufficient to have many blocks of 1s in the binary expansion of t.

Reconstructing c_t

- Introducing complete Gauss integrals, this leads to an approximation of c_t:

$$c_t = \frac{1}{2} + \frac{1}{4\sqrt{\pi}} \left(A_2^{-1/2} + iA_2^{-3/2} A_3 + \frac{3}{4} A_2^{-5/2} \left(2i\,A_5 - A_4 - \frac{i\,A_3}{6} \right) + \frac{15}{8} A_2^{-7/2} \left(\frac{A_3}{2} - 2i\,A_4 \right) A_3 + \frac{35}{16} i\,A_2^{-9/2} A_3^3 \right) + \mathcal{O}(E)\,.$$

- The red terms sometimes almost cancel. Therefore we need more cumulants!
- A closer look at the recurrences for A_j finishes the proof: for $c_t > 1/2$ it is sufficient to have many blocks of 1s in the binary expansion of t.

The message

1. *Adding a constant usually changes the binary sum of digits according to a normal law.*
2. *The sum of digits (weakly) increases more often than not under addition of a constant.*

Moments and cumulants

- In a recently accepted paper I proved the following result.

Theorem (S. 2020+)

Let $\varepsilon > 0$. There exists an $M_0 = M_0(\varepsilon)$ such that for $t \geq 0$ having at least M_0 blocks of $\mathtt{1}$s, we have $c_t > 1/2 - \varepsilon$.

- This is weaker than the corollary to our normal distribution-result!
- The proof uses estimates for the moments of $\delta(j,t)$,

$$m_k(t) = \sum_{j \in \mathbb{Z}} \delta(j,t) j^k.$$

  Depending on ε, an increasing number of moments is used.
- Introducing the logarithm of the CF, we only need the variance for proving the above theorem, and only *four* cumulants for the new result.

Moments and cumulants

- In a recently accepted paper I proved the following result.

Theorem (S. 2020+)

Let $\varepsilon > 0$. There exists an $M_0 = M_0(\varepsilon)$ such that for $t \geq 0$ having at least M_0 blocks of 1s, we have $c_t > 1/2 - \varepsilon$.

- This is weaker than the corollary to our normal distribution-result!
- The proof uses estimates for the moments of $\delta(j,t)$,

$$m_k(t) = \sum_{j\in\mathbb{Z}} \delta(j,t) j^k.$$

  Depending on ε, an increasing number of moments is used.
- Introducing the logarithm of the CF, we only need the variance for proving the above theorem, and only *four* cumulants for the new result.

Moments and cumulants

- In a recently accepted paper I proved the following result.

Theorem (S. 2020+)

Let $\varepsilon > 0$. There exists an $M_0 = M_0(\varepsilon)$ such that for $t \ge 0$ having at least M_0 blocks of 1*s, we have $c_t > 1/2 - \varepsilon$.*

- This is weaker than the corollary to our normal distribution-result!
- The proof uses estimates for the moments of $\delta(j,t)$,

$$m_k(t) = \sum_{j \in \mathbb{Z}} \delta(j,t) j^k.$$

  Depending on ε, an increasing number of moments is used.
- Introducing the logarithm of the CF, we only need the variance for proving the above theorem, and only *four* cumulants for the new result.

Moments and cumulants

- In a recently accepted paper I proved the following result.

Theorem (S. 2020+)

Let $\varepsilon > 0$. There exists an $M_0 = M_0(\varepsilon)$ such that for $t \geq 0$ having at least M_0 blocks of 1s, we have $c_t > 1/2 - \varepsilon$.

- This is weaker than the corollary to our normal distribution-result!
- The proof uses estimates for the moments of $\delta(j, t)$,

$$m_k(t) = \sum_{j \in \mathbb{Z}} \delta(j, t) j^k.$$

  Depending on ε, an increasing number of moments is used.
- Introducing the logarithm of the CF, we only need the variance for proving the above theorem, and only *four* cumulants for the new result.

Rows in Pascal's triangle

The densities $\delta(j, t)$ are concerned with *columns* in Pascal's triangle. The *rows* behave similar with respect to p-valuation (the picture is invariant under rotation by $2\pi/3$), but they are finite.

Let j and t be nonnegative integers and set

$$\Theta(j, t) = \left| \left\{ \ell \in \{0, \ldots, t\} : 2^{j+1} \nmid \binom{t}{\ell} \right\} \right|.$$

For brevity, we extend $\Theta(\cdot, t)$ to $\mathbb{R}$ by setting $\Theta(j, t) = 0$ for $j < 0$ and $\Theta(x, t) = \Theta(\lfloor x \rfloor, t)$.

Theorem (S.–Wallner 2018)

Assume that $\varepsilon > 0$ and $\lambda > 0$ is an integer. We set $I_\lambda = [2^\lambda, 2^{\lambda+1})$. Then

$$\left| \left\{ t \in I_\lambda : \sup_{u \in \mathbb{R}} \left| \frac{\Theta_2(\lambda - s_2(t) + u, t)}{t + 1} - \Phi\left(\frac{u}{\sqrt{\lambda}}\right) \right| \geq \varepsilon \right\} \right| = \mathcal{O}\left(\frac{2^\lambda}{\sqrt{\lambda}}\right),$$

where the implied constant may depend on ε.

Rows in Pascal's triangle

The densities $\delta(j,t)$ are concerned with *columns* in Pascal's triangle. The *rows* behave similar with respect to p-valuation (the picture is invariant under rotation by $2\pi/3$), but they are finite.
Let j and t be nonnegative integers and set

$$\Theta(j,t) = \left|\left\{\ell \in \{0,\ldots,t\} : 2^{j+1} \nmid \binom{t}{\ell}\right\}\right|.$$

For brevity, we extend $\Theta(\cdot,t)$ to $\mathbb{R}$ by setting $\Theta(j,t)=0$ for $j<0$ and $\Theta(x,t)=\Theta(\lfloor x\rfloor,t)$.

Theorem (S.–Wallner 2018)

Assume that $\varepsilon>0$ and $\lambda>0$ is an integer. We set $I_\lambda=[2^\lambda,2^{\lambda+1})$. Then

$$\left|\left\{t\in I_\lambda : \sup_{u\in\mathbb{R}}\left|\frac{\Theta_2(\lambda-s_2(t)+u,t)}{t+1}-\Phi\left(\frac{u}{\sqrt{\lambda}}\right)\right|\ge\varepsilon\right\}\right| = \mathcal{O}\left(\frac{2^\lambda}{\sqrt{\lambda}}\right),$$

where the implied constant may depend on ε.

SW2018 in a nutshell

The normal distribution appears in Pascal's triangle — not only in the size of the coefficients, but also in their 2-valuation.

Possible extensions

- We hope to prove a sharpening of this theorem by means of cumulants too.
- Cusick proposed his conjecture when he was working on the related *Tu–Deng conjecture* relevant in cryptography. Let k be a positive integer and $1 \le t < 2^k - 1$. Then the conjecture states that

$$\Bigl|\Bigl\{(a,b) \in \{0,\ldots,2^k-2\}^2 : a+b \equiv t \bmod 2^k-1, \\ s_2(a)+s_2(b) < k\Bigr\}\Bigr| \le 2^{k-1}$$

  and is open. Together with Wallner we proved that this conjecture is true in an asymptotic sense, and that it implies Cusick's conjecture.

  $\longrightarrow$ We want to transfer our method to this situation.

Possible extensions

- We hope to prove a sharpening of this theorem by means of cumulants too.
- Cusick proposed his conjecture when he was working on the related *Tu–Deng conjecture* relevant in cryptography. Let k be a positive integer and $1 \le t < 2^k - 1$. Then the conjecture states that

$$\left|\left\{(a,b) \in \{0,\ldots,2^k-2\}^2 : a+b \equiv t \bmod 2^k-1, \quad s_2(a)+s_2(b) < k\right\}\right| \le 2^{k-1}$$

  and is open. Together with Wallner we proved that this conjecture is true in an asymptotic sense, and that it implies Cusick's conjecture.

  $\longrightarrow$ We want to transfer our method to this situation.

Possible extensions

What about adding t repeatedly? Together with T. Stoll we proved the following theorem.

Theorem (S.–Stoll 2020)

Assume that $k_1, \ldots, k_m \in \mathbb{Z}$. There exist n and t such that for $1 \le \ell \le m$,

$$k_\ell = s_2(n + \ell t) - s_2(n).$$

$\longrightarrow$ Every finite sequence of integers, modulo a shift $\sigma \in \mathbb{Z}$, appears as an arithmetic subsequence of s_2.

This generalizes the theorem "The Thue–Morse sequence has full arithmetic complexity": any finite sequence of 0s and 1s appears as an arithmetic subsequence of the Thue–Morse sequence (proved by Avgustinovich, Fon-Der-Flaass, and Frid (2000)).

Possible extensions

What about adding t repeatedly? Together with T. Stoll we proved the following theorem.

Theorem (S.–Stoll 2020)

Assume that $k_1, \ldots, k_m \in \mathbb{Z}$*. There exist* n *and* t *such that for* $1 \le \ell \le m$,

$$k_\ell = s_2(n + \ell t) - s_2(n).$$

$\longrightarrow$ Every finite sequence of integers, modulo a shift $\sigma \in \mathbb{Z}$, appears as an arithmetic subsequence of s_2.

This generalizes the theorem "The Thue–Morse sequence has full arithmetic complexity": any finite sequence of 0s and 1s appears as an arithmetic subsequence of the Thue–Morse sequence (proved by Avgustinovich, Fon-Der-Flaass, and Frid (2000)).

Possible extensions

Study the asymptotic densities

$$\delta(k_1,\ldots,k_m,t)=\mathrm{dens}\Big|\big\{n : s_2(n+\ell t)-s_2(n)=k_\ell \text{ for } 1\le \ell\le m\big\}\Big|$$

and prove multidimensional generalizations of Cusick's conjecture and the limit law.

Possible conjectures involve multidimensional Gaussians and tuples $(s_2(n+\ell t))_{0\le\ell\le m}$ in certain quadrants, octants,... (see [S.–Stoll 2020]).

Thank you!

[1] Supported by the Austrian Science Fund (FWF), Projects F55 and MuDeRa (jointly with ANR).