The digits of $n + t$

Lukas Spiegelhofer[1]

September 29, 2020, Séminaire Ernest

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

The fundamental question

Every nonnegative integer n admits a unique expansion as a finite 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 vector $(\varepsilon_j)_{j\ge 0}$ is the *binary expansion* of n.

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

- Let us begin with $t = 1$. 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.

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

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

The fundamental question

Every nonnegative integer n admits a unique expansion as a finite 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 vector $(\varepsilon_j)_{j\ge 0}$ is the *binary expansion* of n.

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

- Let us begin with $t = 1$. 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.

The fundamental question

Every nonnegative integer n admits a unique expansion as a finite 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 vector $(\varepsilon_j)_{j \ge 0}$ is the *binary expansion* of n.

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

- Let us begin with $t = 1$. 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.

The fundamental question

Every nonnegative integer n admits a unique expansion as a finite 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 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?*

- Let us begin with $t = 1$. 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.

We do not know the answer

For $t = 3$ we have the following cases:

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

- In this manner, we can in principle describe the situation for any given t completely.
- However, we obtain long case distinctions for growing t, and a structural principle describing these cases is unavailable. Conclusion:

  We do not fully understand addition in base 2.
- It is difficult enough to consider the *binary sum-of-digits* $s_2(n)$, which is the number of 1s in the binary expansion of n. ("How many powers of 2 do we need to write n as their sum?")

We do not know the answer

For $t = 3$ we have the following cases:

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

- In this manner, we can in principle describe the situation for any given t completely.
- However, we obtain long case distinctions for growing t, and a structural principle describing these cases is unavailable. Conclusion:

  We do not fully understand addition in base 2.
- It is difficult enough to consider the *binary sum-of-digits* $s_2(n)$, which is the number of 1s in the binary expansion of n. ("How many powers of 2 do we need to write n as their sum?")

We do not know the answer

For $t = 3$ we have the following cases:

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

- In this manner, we can in principle describe the situation for any given t completely.
- However, we obtain long case distinctions for growing t, and a structural principle describing these cases is unavailable. Conclusion:

  We do not fully understand addition in base 2.
- It is difficult enough to consider the *binary sum-of-digits* $s_2(n)$, which is the number of 1s in the binary expansion of n. ("How many powers of 2 do we need to write n as their sum?")

We do not know the answer

For $t = 3$ we have the following cases:

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

- In this manner, we can in principle describe the situation for any given t completely.
- However, we obtain long case distinctions for growing t, and a structural principle describing these cases is unavailable. Conclusion:

  We do not fully understand addition in base 2.
- It is difficult enough to consider the *binary sum-of-digits* $s_2(n)$, which is the number of 1s in the binary expansion of n. ("How many powers of 2 do we need to write n as their sum?")

Two examples

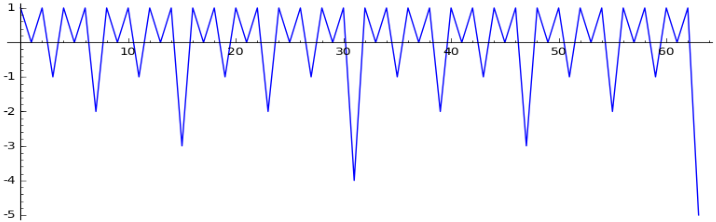


Figure: The *ruler sequence* $s_2(n+1) - s_2(n)$.

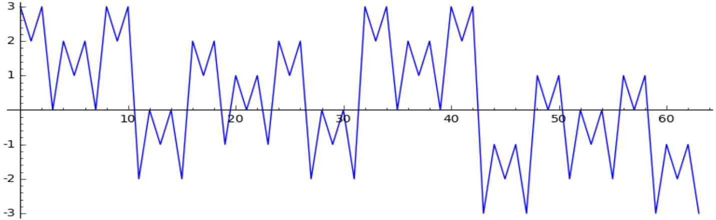


Figure: Some values of $s_2(n+21) - s_2(n)$.

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

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

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

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

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

For example,

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

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

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

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

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

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

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

Densities for Cusick's conjecture

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

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

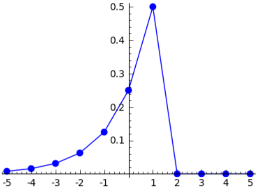
- The densities $\delta(j,t)$ give us a probability distribution on $\mathbb{Z}$ for each t.

Densities for Cusick's conjecture

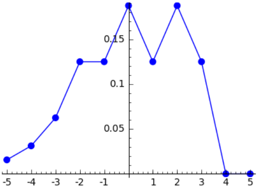
More generally, for integers $t \geq 0$ and j we define

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

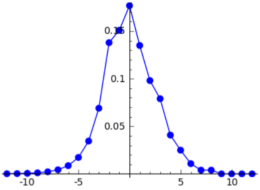
- The densities $\delta(j,t)$ give us a probability distribution on $\mathbb{Z}$ for each t.



$t = 1$



$t = 21$



$t = 999$

A two-dimensional recurrence

The array δ satisfies the recurrence

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

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

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

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

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

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

The first main 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).

The second main 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 main 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! ☕

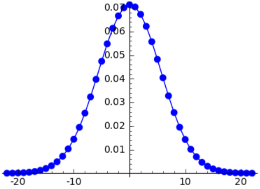
The second main theorem

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

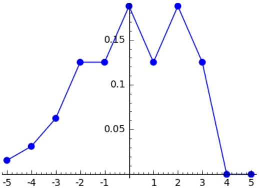
Theorem (S.–Wallner 2020+)

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!



"easy"



hard

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 $\operatorname{Re}\gamma_t(x) > 0$ 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

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

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

for $\vartheta \in D_t$.

- 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

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

valid for ϑ in a certain disk.

Method of proof of the theorems

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

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

for $\vartheta \in D_t$.

- 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

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

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.

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.

Proof of the first main 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 main 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 main 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 main theorem, II

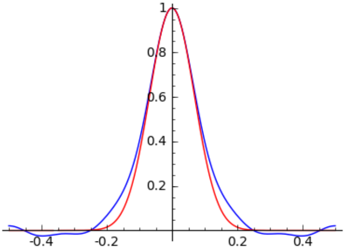


Figure: Illustrating the propositions for $t = 123$.

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

As we noted, 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 $\bigl|\widetilde{\gamma}_t(\vartheta)\bigr| \le CM\vartheta^6$ for $|\vartheta| \le \min\bigl(M^{-1/6}, 1/(4\pi)\bigr)$ 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.
- 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

- 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.
- 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

- 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.
- 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:

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

- In order to compute c_t, we have to keep track of the entire vector $\delta(\cdot, t)$; for the above approximation, we only need the four cumulants $A_2, \ldots, A_5$ (which are given by a recurrence).
- A closer look at the sequences 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:

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

- In order to compute c_t, we have to keep track of the entire vector $\delta(\cdot, t)$; for the above approximation, we only need the four cumulants $A_2, \ldots, A_5$ (which are given by a recurrence).
- A closer look at the sequences 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:

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

- In order to compute c_t, we have to keep track of the entire vector $\delta(\cdot, t)$; for the above approximation, we only need the four cumulants $A_2, \ldots, A_5$ (which are given by a recurrence).
- A closer look at the sequences 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

Adding a constant usually changes the binary sum of digits according to a normal law; moreover, the sum of digits (weakly) increases more often than not.

Pascal's triangle modulo powers of two

The easy case $t = 1$ yields

$$s_2(n+1) - s_2(n) = 1 - \nu_2(n+1),$$

and by summation we obtain

$$\nu_2(n!) = n - s_2(n).$$

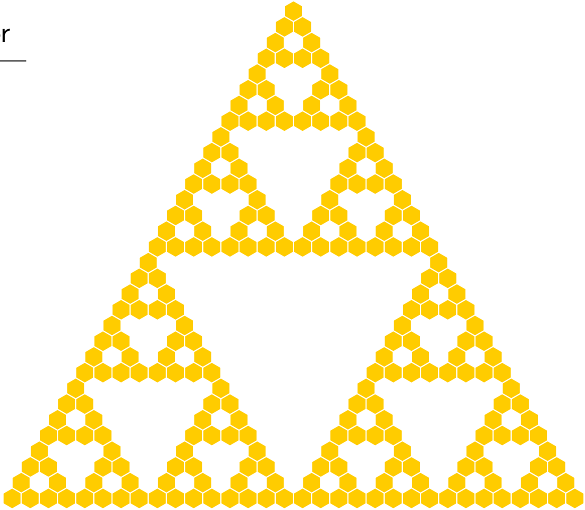
Therefore

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

$\longrightarrow$ we are concerned with divisibility properties of binomial coefficients.
(This is one of my motivations for studying the function s_2.)

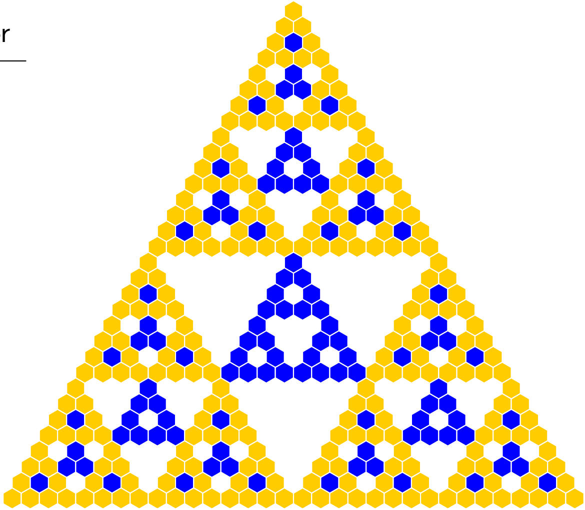
Divisibility of binomial coefficients by powers of two

$\nu_2\binom{n}{t}$	color
0	yellow
1	blue
2	green
3	black
4	green



Divisibility of binomial coefficients by powers of two

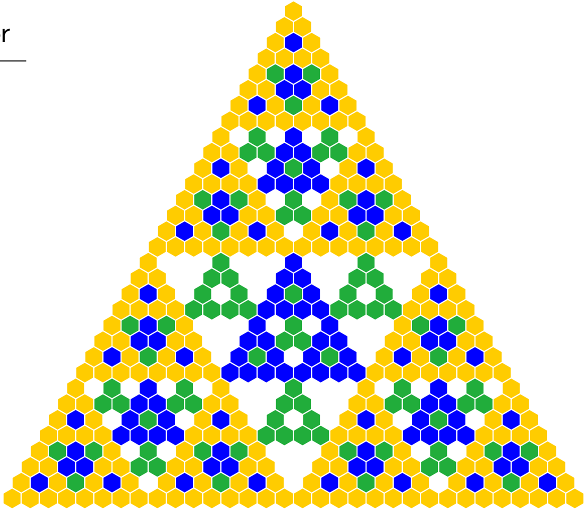
$\nu_2\binom{n}{t}$	color
0	
1	
2	
3	
4	



Rule: "Put a discrete Sierpiński triangle of the next color and of maximal size into each triangular hole."

Divisibility of binomial coefficients by powers of two

$\nu_2\binom{n}{t}$	color
0	yellow hexagon
1	blue hexagon
2	green hexagon
3	black hexagon
4	green hexagon



Rule: "Put a discrete Sierpiński triangle of the next color and of maximal size into each triangular hole."

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.

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.

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 (again by analyzing a trivariate generating function), and that it implies Cusick's conjecture.

  $\longrightarrow$ Can we prove more?

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

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

  and is open. Together with Wallner we proved that this conjecture is true in an asymptotic sense (again by analyzing a trivariate generating function), and that it implies Cusick's conjecture.

  $\longrightarrow$ Can we prove more?

Possible extensions, II

Together with T. Stoll we proved the following theorem.

Theorem (S.–Stoll)

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 the function s_2.

TODO: Study the asymptotic densities

$$\delta(\mathrm{k}, t) = \lim_{N\to\infty} \frac{1}{N} \left| \left\{ n < N : s_2(n + \ell t) - s_2(n) = k_\ell \text{ for } 1 \le \ell \le m \right\} \right|$$

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

Possible extensions, II

Together with T. Stoll we proved the following theorem.

Theorem (S.–Stoll)

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 the function s_2.

TODO: Study the asymptotic densities

$$\delta(\mathrm{k}, t) = \lim_{N \to \infty} \frac{1}{N} \left| \left\{ n < N : s_2(n + \ell t) - s_2(n) = k_\ell \text{ for } 1 \le \ell \le m \right\} \right|$$

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

Thank you! [2]

[2] Supported by the Austrian Science Fund (FWF), Project F55.