

Reciprocals of Binary Power Series

Joshua N. Cooper

Institute of Theoretical Computer Science

Zürich, Switzerland

Dennis Eichhorn

California State University, East Bay

Kevin O'Bryant

City University of New York, College of Staten Island

Research supported by NSF-DMS grants 0202460 and 0303272.



A Few Identities

$$\left(\sum_{n \geq 0} p(n)q^n \right) \left(\sum_{n=-\infty}^{\infty} q^{n(3n-1)/2} \right) \equiv 1 \pmod{2}$$

A Few Identities

$$\left(\sum_{n \geq 0} p(n)q^n \right) \left(\sum_{n=-\infty}^{\infty} q^{n(3n-1)/2} \right) \equiv 1 \pmod{2}$$

$$\left(1 + \sum_{n \geq 0} q^{2^n} \right) \left(\sum_{n \geq 0} q^{2^n - 1} \right) \equiv 1 \pmod{2}$$

A Proof

Let

$$\left(1 + \sum_{n \geq 0} q^{2^n}\right) \left(\sum_{n \geq 0} q^{2^n - 1}\right) = \sum_{k \geq 0} R(k)q^k.$$



A Proof

Let

$$\left(1 + \sum_{n \geq 0} q^{2^n}\right) \left(\sum_{n \geq 0} q^{2^n - 1}\right) = \sum_{k \geq 0} R(k)q^k.$$

If $R(k) > 0$, then

$$k = 2^n + 2^m - 1,$$

and if $n \neq m$

$$k = (2^n) + (2^m - 1) = (2^m) + (2^n - 1),$$

so $R(k) = 2$.



A Proof

Let

$$\left(1 + \sum_{n \geq 0} q^{2^n}\right) \left(\sum_{n \geq 0} q^{2^n - 1}\right) = \sum_{k \geq 0} R(k)q^k.$$

If $R(k) > 0$, then

$$k = 2^n + 2^m - 1,$$

and if $n \neq m$

$$k = (2^n) + (2^m - 1) = (2^m) + (2^n - 1),$$

so $R(k) = 2$.

If $n = m$, then

$$k = (2^n) + (2^m - 1) = (0) + (2^{n+1} - 1),$$

and so $R(k) = 2$.



A Few Identities

$$\left(\sum_{n \geq 0} p(n)q^n \right) \left(\sum_{n=-\infty}^{\infty} q^{3(3n-1)/2} \right) \equiv 1 \pmod{2}$$

$$\left(1 + \sum_{n \geq 0} q^{2^n} \right) \left(\sum_{n \geq 0} q^{2^n - 1} \right) \equiv 1 \pmod{2}$$

$$(1 + q)(1 + q + q^2 + q^3 + \dots) \equiv 1 \pmod{2}$$

A Few Identities

$$\left(\sum_{n \geq 0} p(n)q^n \right) \left(\sum_{n=-\infty}^{\infty} q^{3(3n-1)/2} \right) \equiv 1 \pmod{2}$$

$$\left(1 + \sum_{n \geq 0} q^{2^n} \right) \left(\sum_{n \geq 0} q^{2^n - 1} \right) \equiv 1 \pmod{2}$$

$$(1 + q)(1 + q + q^2 + q^3 + \dots) \equiv 1 \pmod{2}$$

Nonnegative integer sets A and B are reciprocals if their generating functions are reciprocals in $\mathbb{F}_2[[q]]$.

$$A = \{0, 1\}, \quad B = \{0, 1, 2, 3, \dots\}$$

$$A = \{0, 1, 2, 4, 8, 16, \dots\}, \quad B = \{0, 1, 3, 7, 15, \dots\}$$

What it means

Suppose

$$(1 + a_1q + a_2q^2 + \cdots) (1 + b_1q + b_2q^2 + \cdots) = 1.$$

What it means

Suppose

$$(1 + a_1q + a_2q^2 + \cdots) (1 + b_1q + b_2q^2 + \cdots) = 1.$$

The coefficient of q^n is

$$b_n + b_{n-1}a_1 + b_{n-2}a_2 + \cdots + b_2a_{n-2} + b_1a_{n-1} + a_n = 0.$$



What it means

Suppose

$$(1 + a_1q + a_2q^2 + \cdots) (1 + b_1q + b_2q^2 + \cdots) = 1.$$

The coefficient of q^n is

$$b_n + b_{n-1}a_1 + b_{n-2}a_2 + \cdots + b_2a_{n-2} + b_1a_{n-1} + a_n = 0.$$

Remark: For every set A there is a B such that...



Suppose

$$(1 + a_1q + a_2q^2 + \cdots) (1 + b_1q + b_2q^2 + \cdots) = 1.$$

The coefficient of q^n is

$$b_n + b_{n-1}a_1 + b_{n-2}a_2 + \cdots + b_2a_{n-2} + b_1a_{n-1} + a_n = 0.$$

Remark: For every set A there is a B such that...

Remark: $\mathcal{F} \in \mathbb{F}_2[[q]]$ is invertible if and only if...

Special Case: Finite Sets

If $\max A = d$, then

$$b_n = b_{n-1}a_1 + b_{n-2}a_2 + \cdots + b_{n-d}a_d.$$

The sequence (b) is a linear recurrence sequence with boundary $b_0 = 1$,
 $b_{-1} = 0$, $b_{-2} = 0$, \dots



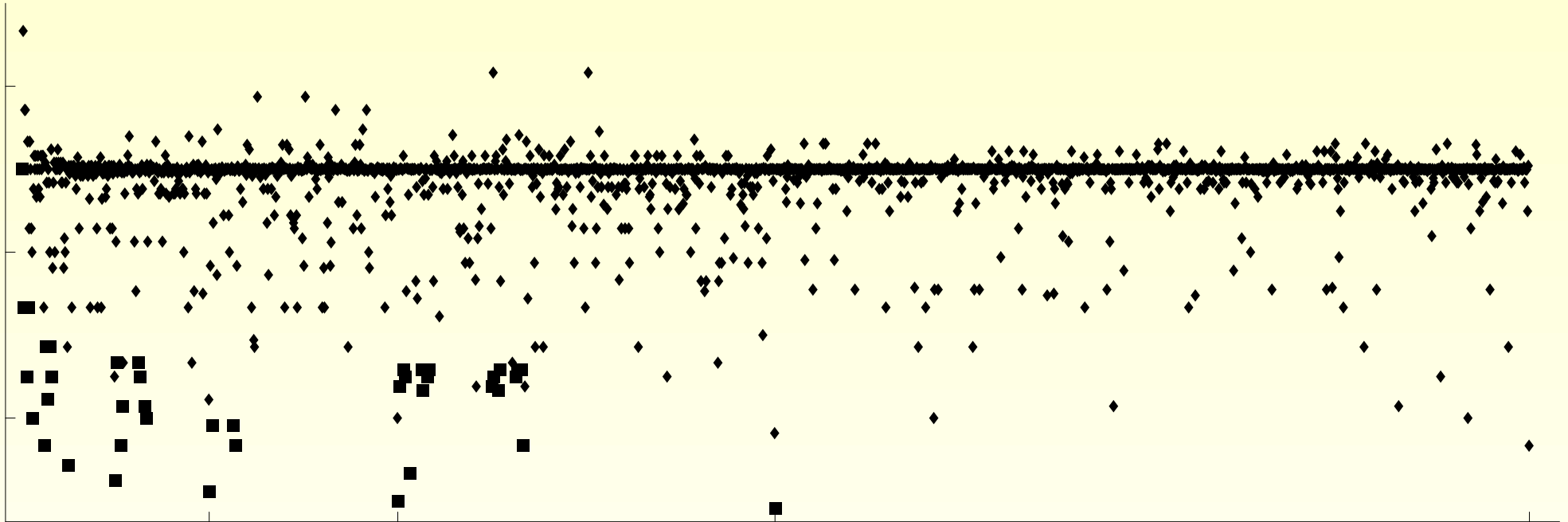
If $\max A = d$, then

$$b_n = b_{n-1}a_1 + b_{n-2}a_2 + \cdots + b_{n-d}a_d.$$

The sequence (b) is a linear recurrence sequence with boundary $b_0 = 1$, $b_{-1} = 0$, $b_{-2} = 0$, \dots

- (b) is periodic.
- (b) may have more 0 than 1 (when d is small)
- If q generates the multiplicative group of $\mathbb{F}_2[q]/(\mathcal{A})$, then every binary word of length d appears in (b) except $0000 \cdots 000$. This is called a reduced de Bruijn cycle.
- Period length = $2^d - 1$, with 2^{d-1} ones. Density slightly larger than $1/2$.

Statistical Imagery



The points $(n, \delta(\bar{\mathcal{P}}_n))$, where the coeffs of \mathcal{P}_n are the binary expansion of n .

Questions

- What are the possible densities of reciprocals of finite sets?
- Is the bias toward $< 1/2$ a law of small numbers?

Theorems

If $\mathcal{P}(q)$ is a polynomial, then there is another polynomial \mathcal{P}^* and a positive integer D such that $\mathcal{P}\mathcal{P}^* = 1 + q^D$. We call the minimal such D the order of \mathcal{P} .



Theorems

If $\mathcal{P}(q)$ is a polynomial, then there is another polynomial \mathcal{P}^* and a positive integer D such that $\mathcal{P}\mathcal{P}^* = 1 + q^D$. We call the minimal such D the order of \mathcal{P} .

Theorem: If \mathcal{P} has degree d and order $2^d - 1$, then

$$\delta(\bar{\mathcal{P}}) = \frac{2^{d-1}}{2^d - 1}.$$



Theorems

If $\mathcal{P}(q)$ is a polynomial, then there is another polynomial \mathcal{P}^* and a positive integer D such that $\mathcal{P}\mathcal{P}^* = 1 + q^D$. We call the minimal such D the order of \mathcal{P} .

Theorem: If \mathcal{P} has degree d and order $2^d - 1$, then

$$\delta(\bar{\mathcal{P}}) = \frac{2^{d-1}}{2^d - 1}.$$

Theorem: If \mathcal{P} has order larger than 3, then

$$\min\{\delta(\bar{\mathcal{P}}), \delta(\bar{\mathcal{P}}^*)\} \leq \frac{1}{2}.$$



Theorems

If $\mathcal{P}(q)$ is a polynomial, then there is another polynomial \mathcal{P}^* and a positive integer D such that $\mathcal{P}\mathcal{P}^* = 1 + q^D$. We call the minimal such D the order of \mathcal{P} .

Theorem: If \mathcal{P} has degree d and order $2^d - 1$, then

$$\delta(\bar{\mathcal{P}}) = \frac{2^{d-1}}{2^d - 1}.$$

Theorem: If \mathcal{P} has order larger than 3, then

$$\min\{\delta(\bar{\mathcal{P}}), \delta(\bar{\mathcal{P}}^*)\} \leq \frac{1}{2}.$$

Proposition: The reciprocal of an eventually periodic set is one too.

Quadratic Sequences

$$\Theta(c_1, c_2) := \left\{ c_1 n + c_2 \frac{n(n-1)}{2} : n \in \mathbb{Z} \right\}$$

Quadratic Sequences

$$\Theta(c_1, c_2) := \left\{ c_1 n + c_2 \frac{n(n-1)}{2} : n \in \mathbb{Z} \right\}$$

WOLOG: $\gcd(c_1, c_2) = 1, 0 \leq 2c_1 \leq c_2$

Quadratic Sequences

$$\Theta(c_1, c_2) := \left\{ c_1 n + c_2 \frac{n(n-1)}{2} : n \in \mathbb{Z} \right\}$$

WOLOG: $\gcd(c_1, c_2) = 1, 0 \leq 2c_1 \leq c_2$

$$\Theta(0, 1) = \left\{ \binom{n}{2} : n \geq 1 \right\}$$

$$\Theta(1, 2) = \{n^2 : n \geq 0\}$$

$$\Theta(1, 3) = \{\text{pentagonals}\}$$



The Experimental Density of the Inverse of a Quadratic Sequence

		c_1					
		1	2	3	4	5	6
c_2	2	2090					
	3	5004					
	4	5088					
	5	5057	5019				
	6	2114					
	7	5020	5023	5000			
	8	5002		5045			
	9	5085	4942		4994		
	10	3854		4062			
	11	4994	4959	5073	4982	5039	
	12	5044				5073	
	13	4985	5002	4973	5071	4963	5090
	14	4391		4445		4109	

The Experimental Density of the Inverse of a Quadratic Sequence

		c_1					
		1	2	3	4	5	6
c_2	2	2090					
	3	5004					
	4	5088					
	5	5057	5019				
	6	2114					
	7	5020	5023	5000			
	8	5002		5045			
	9	5085	4942		4994		
	10	3854		4062			
	11	4994	4959	5073	4982	5039	
	12	5044				5073	
	13	4985	5002	4973	5071	4963	5090
	14	4391		4445		4109	

A Grand Conjecture

The reciprocal of the set $\Theta(c_1, c_2)$, where $0 \leq 2c_1 \leq c_2$ and $\gcd(c_1, c_2) = 1$, has density 0 if $c_2 \equiv 2 \pmod{4}$, and otherwise has density $1/2$.

More precisely, if $c_2 \equiv 2 \pmod{4}$, then

$$\lim_{n \rightarrow \infty} \frac{|\overline{\Theta(c_1, c_2)} \cap [0, n]|}{n / \log n} = C,$$

for some positive constant C depending only on c_2 . If $c_2 \not\equiv 2 \pmod{4}$, then

$$\limsup_{n \rightarrow \infty} \left| \frac{|\overline{\Theta(c_1, c_2)} \cap [0, n]| - n/2}{\sqrt{n \log \log(n)}/2} \right| = 1.$$

Two Modest Conjectures

How many numbers less than N can be written in the form

$$x_0^2 + 2x_1^2 + 4x_2^2 + 8x_3^2 + 16x_4^2 + \cdots ,$$

with nonnegative x_i , in an odd number of ways?

Two Modest Conjectures

How many numbers less than N can be written in the form

$$x_0^2 + 2x_1^2 + 4x_2^2 + 8x_3^2 + 16x_4^2 + \cdots ,$$

with nonnegative x_i , in an odd number of ways?

Conjecture: $\sim \frac{2N}{\log N}$.

We know except for $n \equiv 3 \pmod{4}$.



Two Modest Conjectures

How many numbers less than N can be written in the form

$$x_0^2 + 2x_1^2 + 4x_2^2 + 8x_3^2 + 16x_4^2 + \cdots ,$$

with nonnegative x_i , in an odd number of ways?

Conjecture: $\sim \frac{2N}{\log N}$.

We know except for $n \equiv 3 \pmod{4}$.

Conjecture: $\#\{n \leq N : p(n) \text{ is odd}\} \sim \frac{N}{2}$.



Two Modest Conjectures

How many numbers less than N can be written in the form

$$x_0^2 + 2x_1^2 + 4x_2^2 + 8x_3^2 + 16x_4^2 + \cdots,$$

with nonnegative x_i , in an odd number of ways?

Conjecture: $\sim \frac{2N}{\log N}$.

We know except for $n \equiv 3 \pmod{4}$.

Conjecture: $\#\{n \leq N : p(n) \text{ is odd}\} \sim \frac{N}{2}$.

Current bests:

$$\# \geq \left(\frac{\pi^2 \sqrt{3}}{2} - o(1) \right) \frac{\sqrt{N}}{\log N} \quad (\text{D. Eichhorn})$$
$$\lim_{N \rightarrow \infty} \frac{N - \#}{\sqrt{N}} = \infty \quad (\text{Serre})$$



Typical Behavior

Let f_1, f_2, \dots be independent binary random variables, with

$$\mathbb{P}[f_n = 0]\mathbb{P}[f_n = 1]$$

bounded away from 0.

Define $\bar{f}_1, \bar{f}_2, \dots$ by

$$(1 + f_1q + f_2q^2 + f_3q^3 + \dots)(1 + \bar{f}_1q + \bar{f}_2q^2 + \bar{f}_3q^3 + \dots) = 1.$$

Then the number of $\bar{f}_1, \bar{f}_2, \dots, \bar{f}_N$ that are 1 is $\sim N/2$ with probability 1.

Explanation

$$\bar{f}_n = \sum_{\vec{x}} f_{x_1} f_{x_2} \cdots f_{x_\ell}$$

where the summation extends over all tuples $\vec{x} = (x_1, \dots, x_\ell)$ with $n = \sum_{i=1}^{\ell} x_i$ and each $x_i > 0$ (ℓ is allowed to vary).



Explanation

$$\bar{f}_n = \sum_{\vec{x}} f_{x_1} f_{x_2} \cdots f_{x_\ell}$$

where the summation extends over all tuples $\vec{x} = (x_1, \dots, x_\ell)$ with $n = \sum_{i=1}^{\ell} x_i$ and each $x_i > 0$ (ℓ is allowed to vary).

$$\bar{f}_n = f_n + f_{n-2i} \bar{f}_i + f_{n-4i} \bar{f}_2 + \dots + f_{n/2} \bar{f}_{n/4} + \textit{mess}$$

and *mess* depends only on $f_1, f_2, \dots, f_{n/2-1}$.



Thus,

$$H[f_n | f_1, \dots, f_{n/2-1}] \geq H[\sum_{i \in A} f_i | A]$$

where $A = \{n - 2i : 0 \leq i < n/4, \bar{f}_i = 1\}$. Since

- $|A| \rightarrow \infty$ (requires easy proof),
- this uncertainty goes to $1/2$ (requires proof),
- and so $\mathbb{P}[f_n = 0] \rightarrow 1/2$ (obvious),
- and consequently $\#\{n \leq N : \bar{f}_n = 0\} \sim N/2$ (obscure Borel-Cantelli Lemma)

Thus,

$$H[f_n | f_1, \dots, f_{n/2-1}] \geq H[\sum_{i \in A} f_i | A]$$

where $A = \{n - 2i : 0 \leq i < n/4, \bar{f}_i = 1\}$. Since

- $|A| \rightarrow \infty$ (requires easy proof),
- this uncertainty goes to $1/2$ (requires proof),
- and so $\mathbb{P}[f_n = 0] \rightarrow 1/2$ (obvious),
- and consequently $\#\{n \leq N : \bar{f}_n = 0\} \sim N/2$ (obscure Borel-Cantelli Lemma)

Thus,

$$H[f_n | f_1, \dots, f_{n/2-1}] \geq H[\sum_{i \in A} f_i | A]$$

where $A = \{n - 2i : 0 \leq i < n/4, \bar{f}_i = 1\}$. Since

- $|A| \rightarrow \infty$ (requires easy proof),
- this uncertainty goes to $1/2$ (requires proof),
- and so $\mathbb{P}[f_n = 0] \rightarrow 1/2$ (obvious),
- and consequently $\#\{n \leq N : \bar{f}_n = 0\} \sim N/2$ (obscure Borel-Cantelli Lemma)

Thus,

$$H[f_n | f_1, \dots, f_{n/2-1}] \geq H[\sum_{i \in A} f_i | A]$$

where $A = \{n - 2i : 0 \leq i < n/4, \bar{f}_i = 1\}$. Since

- $|A| \rightarrow \infty$ (requires easy proof),
- this uncertainty goes to $1/2$ (requires proof),
- and so $\mathbb{P}[f_n = 0] \rightarrow 1/2$ (obvious),
- and consequently $\#\{n \leq N : \bar{f}_n = 0\} \sim N/2$ (obscure Borel-Cantelli Lemma)

Thus,

$$H[f_n | f_1, \dots, f_{n/2-1}] \geq H[\sum_{i \in A} f_i | A]$$

where $A = \{n - 2i : 0 \leq i < n/4, \bar{f}_i = 1\}$. Since

- $|A| \rightarrow \infty$ (requires easy proof),
- this uncertainty goes to $1/2$ (requires proof),
- and so $\mathbb{P}[f_n = 0] \rightarrow 1/2$ (obvious),
- and consequently $\#\{n \leq N : \bar{f}_n = 0\} \sim N/2$ (obscure Borel-Cantelli Lemma)

Plans for future development:

- Take some interesting set of integers, call it A . Find \bar{A} .
- Probabilistic argument is not most general possible.
- [arXiv:math.NT/0506496](https://arxiv.org/abs/math/0506496)

Conclusion

Plans for future development:

- Take some interesting set of integers, call it A . Find \bar{A} .
- Probabilistic argument is not most general possible.
- [arXiv:math.NT/0506496](https://arxiv.org/abs/math/0506496)



Conclusion

Plans for future development:

- Take some interesting set of integers, call it A . Find \bar{A} .
- Probabilistic argument is not most general possible.
- [arXiv:math.NT/0506496](https://arxiv.org/abs/math/0506496)



Conclusion

Plans for future development:

- Take some interesting set of integers, call it A . Find \bar{A} .
- Probabilistic argument is not most general possible.
- [arXiv:math.NT/0506496](https://arxiv.org/abs/math/0506496)



Plans for future development:

- Take some interesting set of integers, call it A . Find \bar{A} .
- Probabilistic argument is not most general possible.
- [arXiv:math.NT/0506496](https://arxiv.org/abs/math/0506496)

The End