Hamming Weight of the Non-Adjacent-Form under Various Input Statistics and a Two-Dimensional Version of Hwang's Quasi-Power-Theorem

Clemens Heuberger

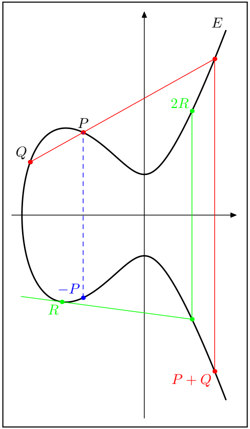
Graz University of Technology, Austria
partly based on joint work with
H. Prodinger, Stellenbosch University, South Africa

Supported by the Austrian Science Foundation FWF, project S9606,
that is part of the Austrian National Research Network
"Analytic Combinatorics and Probabilistic Number Theory."

Maresias, AofA 2008, April 16th, 2008

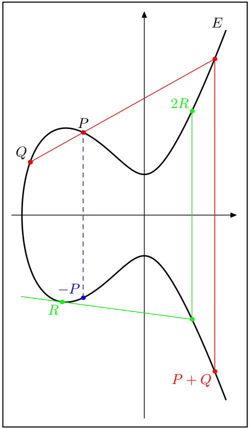
Elliptic curve cryptography

Elliptic Curve $E : y^2 = x^3 + ax^2 + bx + c$
For $P \in E$ and $n \in \mathbb{Z}$, nP can be calculated easily.



Elliptic curve cryptography

Elliptic Curve $E : y^2 = x^3 + ax^2 + bx + c$
For $P \in E$ and $n \in \mathbb{Z}$, nP can be calculated easily.
No efficient algorithm to calculate n from P and nP?
Fast calculation of nP desirable!



Double-and-Add Algorithm

Calculating $27P$ via a doubling and adding scheme using the standard binary expansion of 27:

$$\begin{aligned} 27 &= (11011)_2, \\ 27P &= 2(2(2(2(P) + P) + 0) + P) + P. \end{aligned}$$

Double-and-Add Algorithm

Calculating $27P$ via a doubling and adding scheme using the standard binary expansion of 27:

$$\begin{aligned} 27 &= (11011)_2, \\ 27P &= 2(2(2(2(P) + P) + 0) + P) + P. \end{aligned}$$

Number of additions $\sim$ Hamming weight of the binary expansion (Number of nonzero digits)

Double-and-Add Algorithm

Calculating $27P$ via a doubling and adding scheme using the standard binary expansion of 27:

$$\begin{aligned} 27 &= (11011)_2, \\ 27P &= 2(2(2(2(P) + P) + 0) + P) + P. \end{aligned}$$

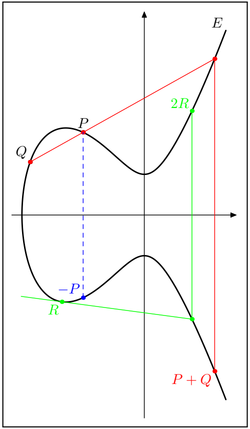
Number of additions $\sim$ Hamming weight of the binary expansion (Number of nonzero digits)
Number of multiplications $\sim$ length of the expansion

Double, Add, and Subtract Algorithm

Subtraction is as cheap as addition!

$$\begin{aligned} 27 &= (100\bar{1}0\bar{1})_2, \\ 27P &= 2(2(2(2(2(P)+0)+0)-P)+0)-P. \end{aligned}$$

$(\bar{1} := -1)$



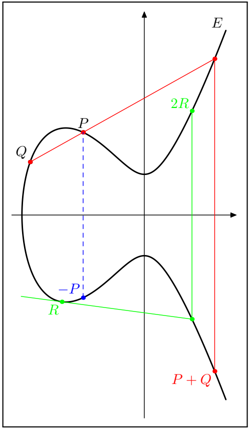
Double, Add, and Subtract Algorithm

Subtraction is as cheap as addition!

$$27 = (100\bar{1}0\bar{1})_2,$$
$$27P = 2(2(2(2(2(P) + 0) + 0) - P) + 0) - P.$$

$(\bar{1} := -1)$

$\Longrightarrow$ Use of signed digit expansions



Double, Add, and Subtract Algorithm

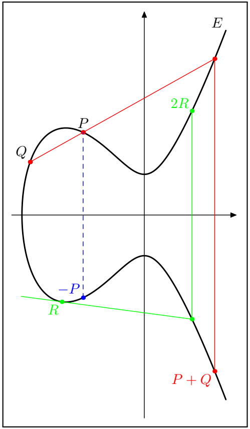
Subtraction is as cheap as addition!

$$27 = (100\bar{1}0\bar{1})_2,$$
$$27P = 2(2(2(2(2(P)+0)+0)-P)+0)-P.$$

$(\bar{1} := -1)$

$\implies$ Use of signed digit expansions

Number of additions/subtractions $\sim$ Hamming weight of the binary expansion



Double, Add, and Subtract Algorithm

Subtraction is as cheap as addition!

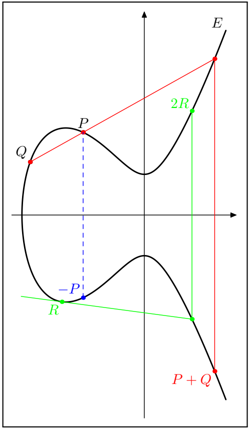
$$27 = (100\bar{1}0\bar{1})_2,$$
$$27P = 2(2(2(2(2(P)+0)+0)-P)+0)-P.$$

$(\bar{1} := -1)$

$\Longrightarrow$ Use of signed digit expansions

Number of additions/subtractions $\sim$ Hamming weight of the binary expansion

Number of multiplications $\sim$ length of the expansion



Double, Add, and Subtract Algorithm

Subtraction is as cheap as addition!

$$27 = (100\bar{1}0\bar{1})_2,$$
$$27P = 2(2(2(2(2(P) + 0) + 0) - P) + 0) - P.$$

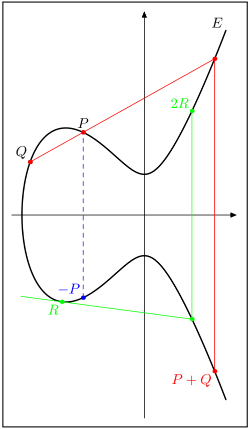
$(\bar{1} := -1)$

$\Longrightarrow$ Use of signed digit expansions

Number of additions/subtractions $\sim$ Hamming weight of the binary expansion

Number of multiplications $\sim$ length of the expansion

There are (infinitely) many signed binary expansions of an integer (Redundancy)



Double, Add, and Subtract Algorithm

Subtraction is as cheap as addition!

$$\begin{aligned} 27 &= (100\bar{1}0\bar{1})_2, \\ 27P &= 2(2(2(2(2(P) + 0) + 0) - P) + 0) - P. \end{aligned}$$

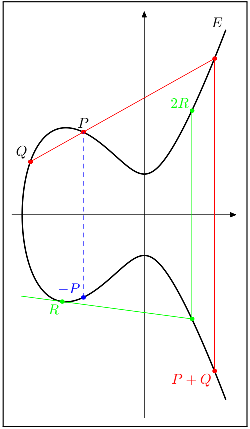
$(\bar{1} := -1)$

$\Longrightarrow$ Use of signed digit expansions

Number of additions/subtractions $\sim$ Hamming weight of the binary expansion

Number of multiplications $\sim$ length of the expansion

There are (infinitely) many signed binary expansions of an integer (Redundancy) $\Longrightarrow$ find expansion of minimal Hamming weight.



Deriving a Low-Weight Representation

Take an integer n.

Deriving a Low-Weight Representation

Take an integer n.

- If n is even, we have to take 0 as least significant digit and continue with $n/2$.

Deriving a Low-Weight Representation

Take an integer n.

- If n is even, we have to take 0 as least significant digit and continue with $n/2$.
- If $n \equiv 1 \pmod 4$, we take 1 as least significant digit and continue with $(n-1)/2$. This is even and guarantees a zero in the next step.

Deriving a Low-Weight Representation

Take an integer n.

- If n is even, we have to take 0 as least significant digit and continue with $n/2$.
- If $n \equiv 1 \pmod 4$, we take 1 as least significant digit and continue with $(n-1)/2$. This is even and guarantees a zero in the next step.
- If $n \equiv 3 \equiv -1 \pmod 4$, we take -1 as least significant digit and continue with $(n+1)/2$. This is even and guarantees a zero in the next step.

Deriving a Low-Weight Representation

Take an integer n.

- If n is even, we have to take 0 as least significant digit and continue with $n/2$.
- If $n \equiv 1 \pmod 4$, we take 1 as least significant digit and continue with $(n-1)/2$. This is even and guarantees a zero in the next step.
- If $n \equiv 3 \equiv -1 \pmod 4$, we take -1 as least significant digit and continue with $(n+1)/2$. This is even and guarantees a zero in the next step.

This procedure yields a zero after every non-zero, which should yield a low weight expansion.

Deriving a Low-Weight Representation

Take an integer n.

- If n is even, we have to take 0 as least significant digit and continue with $n/2$.
- If $n \equiv 1 \pmod 4$, we take 1 as least significant digit and continue with $(n-1)/2$. This is even and guarantees a zero in the next step.
- If $n \equiv 3 \equiv -1 \pmod 4$, we take -1 as least significant digit and continue with $(n+1)/2$. This is even and guarantees a zero in the next step.

This procedure yields a zero after every non-zero, which should yield a low weight expansion. There are no adjacent non-zeros.

Non-Adjacent Form

Theorem (Reitwiesner 1960)

Let $n \in \mathbb{Z}$, then there is exactly one signed binary expansion $\varepsilon \in \{-1, 0, 1\}^{\mathbb{N}_0}$ of n such that

$$n = \sum_{j \geq 0} \varepsilon_j 2^j, \qquad (\varepsilon \text{ is a binary expansion of } n),$$

$$\varepsilon_j \varepsilon_{j+1} = 0 \qquad \text{for all } j \geq 0.$$

It is called the Non-Adjacent Form (NAF) of n.

Non-Adjacent Form

Theorem (Reitwiesner 1960)

Let $n \in \mathbb{Z}$, then there is exactly one signed binary expansion $\varepsilon \in \{-1, 0, 1\}^{\mathbb{N}_0}$ of n such that

$$n = \sum_{j \geq 0} \varepsilon_j 2^j, \qquad (\varepsilon \text{ is a binary expansion of } n),$$

$$\varepsilon_j \varepsilon_{j+1} = 0 \qquad \text{for all } j \geq 0.$$

It is called the Non-Adjacent Form (NAF) of n.
It minimises the Hamming weight amongst all signed binary expansions with digits $\{0, \pm 1\}$ of n.

Non-Adjacent Form: Applications

- Efficient arithmetic operations (Reitwiesner 1960)

Non-Adjacent Form: Applications

- Efficient arithmetic operations (Reitwiesner 1960)
- Coding Theory

Non-Adjacent Form: Applications

- Efficient arithmetic operations (Reitwiesner 1960)
- Coding Theory
- Elliptic Curve Cryptography (Morain and Olivos 1990)

Analysis of the NAF — Known Results

Theorem

$$\mathbb{E}(H_\ell) = \frac{1}{3}\ell + \frac{2}{9} + O(2^{-\ell}),$$

where H_ℓ is the Hamming weight of a random NAF of length $\leq \ell$ (all NAFs of length $\leq \ell$ are considered to be equally likely).

Analysis of the NAF — Known Results

Theorem

$$\mathbb{E}(H_\ell) = \frac{1}{3}\ell + \frac{2}{9} + O(2^{-\ell}),$$
$$\mathbb{V}(H_\ell) = \frac{2}{27}\ell + \frac{8}{81} + O(\ell 2^{-\ell}),$$

where H_ℓ is the Hamming weight of a random NAF of length $\leq \ell$ (all NAFs of length $\leq \ell$ are considered to be equally likely).

Analysis of the NAF — Known Results

Theorem

$$\mathbb{E}(H_\ell) = \frac{1}{3}\ell + \frac{2}{9} + O(2^{-\ell}),$$

$$\mathbb{V}(H_\ell) = \frac{2}{27}\ell + \frac{8}{81} + O(\ell 2^{-\ell}),$$

$$\lim_{\ell\to\infty} \mathbb{P}\left(H_\ell \le \frac{\ell}{3} + h\sqrt{\frac{2\ell}{27}}\right) = \frac{1}{\sqrt{2\pi}} \int_0^h e^{-t^2/2}\, dt,$$

where H_ℓ is the Hamming weight of a random NAF of length $\le \ell$ (all NAFs of length $\le \ell$ are considered to be equally likely).

A Note on Probabilistic Models

There are other probabilistic models:

A Note on Probabilistic Models

There are other probabilistic models:

- Random NAF whose corresponding standard binary expansion has length $\leq \ell$,

A Note on Probabilistic Models

There are other probabilistic models:

- Random NAF whose corresponding standard binary expansion has length $\leq \ell$,
- Random NAF of length $\leq \ell$ where all residue classes modulo 2^ℓ have the same probability.

A Note on Probabilistic Models

There are other probabilistic models:

- Random NAF whose corresponding standard binary expansion has length $\leq \ell$,
- Random NAF of length $\leq \ell$ where all residue classes modulo 2^ℓ have the same probability.
  For instance, 101 and $\bar{1}01$ represent the same residue class modulo 2^3.

Subblock Occurrences without Restricting to Full Blocks

Let $\mathbf{b} = (b_{r-1}, \ldots, b_0) \neq \mathbf{0}$ be an admissible block,
$(\ldots \varepsilon_2(n)\varepsilon_1(n)\varepsilon_0(n))$ the NAF of n.

Subblock Occurrences without Restricting to Full Blocks

Let $\mathbf{b} = (b_{r-1}, \ldots, b_0) \neq \mathbf{0}$ be an admissible block,
$(\ldots \varepsilon_2(n)\varepsilon_1(n)\varepsilon_0(n))$ the NAF of n.
We consider

$$S_{\mathbf{b}}(N) := \sum_{n<N} \sum_{k=0}^{\infty} [(\varepsilon_{k+r-1}(n), \ldots, \varepsilon_k(n)) = \mathbf{b}],$$

i.e. the number of occurrences of the block **b** in the NAFs of the positive integers less than N.

Subblock Occurrences

Theorem (Grabner-H.-Prodinger 2003)

If $b_{r-1} = 0$, *then* $S_{\mathbf{b}}(N) =$

$$\frac{Q(b_0)}{3 \cdot 2^r} N \log_2 N + N h_0(\mathbf{b}) + N H_{\mathbf{b}}(\log_2 N) + o(N),$$

Subblock Occurrences

Theorem (Grabner-H.-Prodinger 2003)

If $b_{r-1} = 0$*, then* $S_{\mathbf{b}}(N) =$

$$\frac{Q(b_0)}{3 \cdot 2^r} N \log_2 N + N h_0(\mathbf{b}) + N H_{\mathbf{b}}(\log_2 N) + o(N),$$

where

$$Q(\eta) = 2 + 2\,[\eta = 0]$$

$$H_{\mathbf{b}}(x) = \sum_{k \in \mathbb{Z} \setminus \{0\}} h_k(\mathbf{b}) e^{2k\pi i x}$$

for explicitly known constants $h_k(\mathbf{b})$*,* $k \in \mathbb{Z}$*.*

Subblock Occurrences

Theorem (Grabner-H.-Prodinger 2003)

If $b_{r-1} = 0$, then $S_{\mathbf{b}}(N) =$

$$\frac{Q(b_0)}{3 \cdot 2^r} N \log_2 N + N h_0(\mathbf{b}) + N H_{\mathbf{b}}(\log_2 N) + o(N),$$

where

$$Q(\eta) = 2 + 2\,[\eta = 0]$$
$$H_{\mathbf{b}}(x) = \sum_{k \in \mathbb{Z} \setminus \{0\}} h_k(\mathbf{b}) e^{2k\pi i x}$$

for explicitly known constants $h_k(\mathbf{b})$, $k \in \mathbb{Z}$.
$H_{\mathbf{b}}(x)$ is a 1-periodic continuous function.

NAF: Counting Subblocks — Explicit constants

$$h_k(\mathbf{b}) = \frac{\zeta\left(\frac{2k\pi i}{\log 2}, \alpha_{\min}(\mathbf{b})\right) - \zeta\left(\frac{2k\pi i}{\log 2}, \alpha_{\max}(\mathbf{b})\right)}{2k\pi i(1 + \frac{2k\pi i}{\log 2})} \quad \text{for } k \neq 0,$$

$$h_0(\mathbf{b}) = \log_2 \Gamma(\alpha_{\min}(\mathbf{b})) - \log_2 \Gamma(\alpha_{\max}(\mathbf{b})) - \frac{Q(b_0)}{3 \cdot 2^r}\left(r + \frac{1}{6} + \frac{1}{\log 2}\right) + \frac{1}{3 \cdot 2^{r-1}},$$

$$\alpha_{\min}(\mathbf{b}) = [\mathrm{value}(\mathbf{b}) < 0] + 2^{-r}\mathrm{value}(\mathbf{b}) - \frac{1 + [b_0 \text{ even}]}{3 \cdot 2^r}$$

$$\alpha_{\max}(\mathbf{b}) = [\mathrm{value}(\mathbf{b}) < 0] + 2^{-r}\mathrm{value}(\mathbf{b}) + \frac{1 + [b_0 \text{ even}]}{3 \cdot 2^r}$$

$\zeta(s, x)$ denotes the Hurwitz ζ-function.

NAF: Counting Subblocks — Explicit constants

$$
\begin{aligned}
h_k(\mathbf{b}) &= \frac{\zeta\left(\frac{2k\pi i}{\log 2}, \alpha_{\min}(\mathbf{b})\right) - \zeta\left(\frac{2k\pi i}{\log 2}, \alpha_{\max}(\mathbf{b})\right)}{2k\pi i(1+\frac{2k\pi i}{\log 2})} \text{ for } k \neq 0,\\
h_0(\mathbf{b}) &= \log_2 \Gamma(\alpha_{\min}(\mathbf{b})) - \log_2 \Gamma(\alpha_{\max}(\mathbf{b}))\\
&\qquad - \frac{Q(b_0)}{3\cdot 2^r}\left(r + \frac{1}{6} + \frac{1}{\log 2}\right) + \frac{1}{3\cdot 2^{r-1}},\\
\alpha_{\min}(\mathbf{b}) &= [\mathrm{value}(\mathbf{b}) < 0] + 2^{-r}\mathrm{value}(\mathbf{b}) - \frac{1+[b_0 \text{ even}]}{3\cdot 2^r}\\
\alpha_{\max}(\mathbf{b}) &= [\mathrm{value}(\mathbf{b}) < 0] + 2^{-r}\mathrm{value}(\mathbf{b}) + \frac{1+[b_0 \text{ even}]}{3\cdot 2^r}
\end{aligned}
$$

$\zeta(s,x)$ denotes the Hurwitz ζ-function.
The case $r=1$ is contained in Thuswaldner (1999).

When does the NAF really have an advantage?

Suggestions by various authors:

- If the standard binary expansion of n has low Hamming weight, there is not much room for improvement of the Hamming weight.

When does the NAF really have an advantage?

Suggestions by various authors:

- If the standard binary expansion of n has low Hamming weight, there is not much room for improvement of the Hamming weight. So it might be desirable to keep the standard binary expansion.

When does the NAF really have an advantage?

Suggestions by various authors:

- If the standard binary expansion of n has low Hamming weight, there is not much room for improvement of the Hamming weight. So it might be desirable to keep the standard binary expansion.
- If, on the other hand, the Hamming weight of the standard binary expansion has very high Hamming weight,

When does the NAF really have an advantage?

Suggestions by various authors:

- If the standard binary expansion of n has low Hamming weight, there is not much room for improvement of the Hamming weight. So it might be desirable to keep the standard binary expansion.
- If, on the other hand, the Hamming weight of the standard binary expansion has very high Hamming weight, the ones' complement of n has low Hamming weight and could be used:

$$n = \sum_{j=0}^{\ell-1} \varepsilon_j 2^j = 2^\ell - \sum_{j=0}^{\ell-1} (1-\varepsilon_j) 2^j - 1$$

  The weight of this new expansion is $\ell + 2 - h$, where h is the weight of the standard binary expansion.

Relation Between Weights

- So, for given input weight (i.e., Hamming weight of the standard binary expansion), what is the expected Hamming weight of the NAF?

Relation Between Weights

- So, for given input weight (i.e., Hamming weight of the standard binary expansion), what is the expected Hamming weight of the NAF?
- How are the weight of the standard expansion and the weight of the NAF related?

Outline of the Remaining Talk

1. Signed Digit Expansions in Cryptography

Outline of the Remaining Talk

1. Signed Digit Expansions in Cryptography
2. Given Input Weight

Outline of the Remaining Talk

Outline of the Remaining Talk

Fixed Input Weight/Length Ratio

Theorem

Let $0 < c < d < 1$ be real numbers. Then the expected Hamming weight of the NAF of a nonnegative integer less than 2^n with unsigned binary digit expansion of Hamming weight k is asymptotically

$$\sim \frac{1 - 4\left(\frac{k}{n} - \frac{1}{2}\right)^2}{3 + 4\left(\frac{k}{n} - \frac{1}{2}\right)^2} n,$$

uniformly for $c \leq k/n \leq d$.

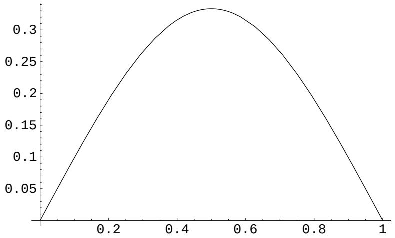
Fixed Input Weight/Length Ratio

Theorem

Let $0 < c < d < 1$ be real numbers. Then the expected Hamming weight of the NAF of a nonnegative integer less than 2^n with unsigned binary digit expansion of Hamming weight k is asymptotically

$$\sim \frac{1-4\left(\frac{k}{n}-\frac{1}{2}\right)^2}{3+4\left(\frac{k}{n}-\frac{1}{2}\right)^2} n,$$

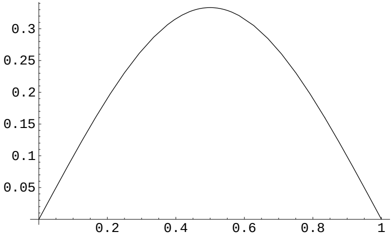
uniformly for $c \leq k/n \leq d$.



$$f(x) = \frac{1-4\left(x-\frac{1}{2}\right)^2}{3+4\left(x-\frac{1}{2}\right)^2}$$

Comments

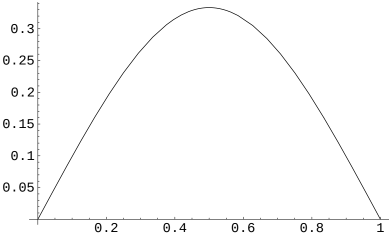
Maximum at $k/n = 1/2$:
Density $1/3$.



$$f(x) = \frac{1 - 4\left(x - \frac{1}{2}\right)^2}{3 + 4\left(x - \frac{1}{2}\right)^2}$$

Comments

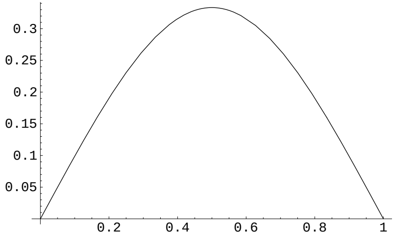
Maximum at $k/n = 1/2$:
Density $1/3$.
This is also the average density without any restriction on the input weight.



$$f(x) = \frac{1 - 4\left(x - \frac{1}{2}\right)^2}{3 + 4\left(x - \frac{1}{2}\right)^2}$$

Comments

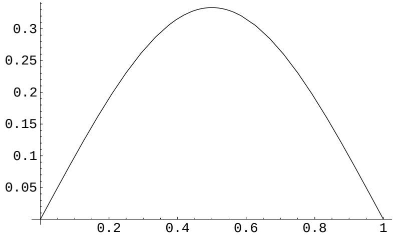
Maximum at $k/n = 1/2$: Density $1/3$.
This is also the average density without any restriction on the input weight.
Reason: There are especially many standard binary expansions of length $\leq n$ of weight $\approx n/2$, namely $\binom{n}{\lfloor n/2 \rfloor}$.



$$f(x) = \frac{1 - 4\left(x - \frac{1}{2}\right)^2}{3 + 4\left(x - \frac{1}{2}\right)^2}$$

Comments

Maximum at $k/n = 1/2$: Density $1/3$.
This is also the average density without any restriction on the input weight.
Reason: There are especially many standard binary expansions of length $\leq n$ of weight $\approx n/2$, namely $\binom{n}{\lfloor n/2 \rfloor}$.
For small or large k/n, the density of the NAF decreases.



$$f(x) = \frac{1 - 4\left(x - \frac{1}{2}\right)^2}{3 + 4\left(x - \frac{1}{2}\right)^2}$$

Idea of the Proof (1)

Let $a_{k\ell n}$ be the number of nonnegative integers whose unsigned binary expansion has length $\leq n$ and Hamming weight k and whose NAF has Hamming weight ℓ.

Idea of the Proof (1)

Let $a_{k\ell n}$ be the number of nonnegative integers whose unsigned binary expansion has length $\leq n$ and Hamming weight k and whose NAF has Hamming weight ℓ. We consider the generating function

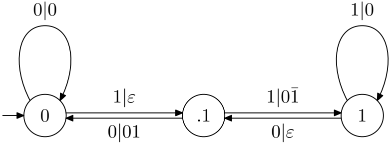
$$G(x, y, z) = \sum_{k,\ell,n \geq 0} a_{k,\ell,n} x^k y^\ell z^n.$$

Idea of the Proof (1)

Let $a_{k\ell n}$ be the number of nonnegative integers whose unsigned binary expansion has length $\leq n$ and Hamming weight k and whose NAF has Hamming weight ℓ. We consider the generating function

$$G(x, y, z) = \sum_{k,\ell,n\geq 0} a_{k,\ell,n} x^k y^\ell z^n.$$

Consider the transducer automaton



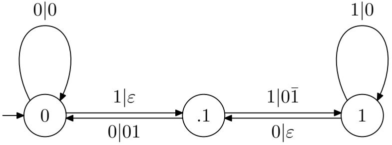
converting the standard binary expansion to the NAF.

Idea of the Proof (1)

Let $a_{k\ell n}$ be the number of nonnegative integers whose unsigned binary expansion has length $\le n$ and Hamming weight k and whose NAF has Hamming weight ℓ. We consider the generating function

$$G(x,y,z) = \sum_{k,\ell,n\ge 0} a_{k,\ell,n} x^k y^\ell z^n.$$

Consider the transducer automaton



converting the standard binary expansion to the NAF. This yields

$$G(x,y,z) = \frac{x^2y^2z^2 - x^2yz^2 - xyz^2 - xz + xyz + 1}{x^2yz^3 + xyz^3 + xz^2 - 2xyz^2 - xz - z + 1}.$$

Idea of the Proof (2)

$$G(x,y,z) = \sum_{k,\ell,n\geq 0} a_{k,\ell,n} x^k y^\ell z^n = \frac{x^2y^2z^2 - x^2yz^2 - xyz^2 - xz + xyz + 1}{x^2yz^3 + xyz^3 + xz^2 - 2xyz^2 - xz - z + 1}.$$

Idea of the Proof (2)

$$G(x,y,z) = \sum_{k,\ell,n\geq 0} a_{k,\ell,n} x^k y^\ell z^n$$
$$= \frac{x^2y^2z^2 - x^2yz^2 - xyz^2 - xz + xyz + 1}{x^2yz^3 + xyz^3 + xz^2 - 2xyz^2 - xz - z + 1}.$$

Taking the derivative w.r.t. y and setting $y = 1$ yields

$$\frac{\partial}{\partial y} G(x,y,z)\Big|_{y=1} = \sum_{k,\ell,n\geq 0} \ell a_{k,\ell,n} x^k z^n = \frac{xz\left(x^2z^2 + xz^2 - 1\right)}{(xz+z-1)^2\left(xz^2-1\right)}.$$

Idea of the Proof (2)

$$G(x,y,z) = \sum_{k,\ell,n\geq 0} a_{k,\ell,n} x^k y^\ell z^n$$
$$= \frac{x^2y^2z^2 - x^2yz^2 - xyz^2 - xz + xyz + 1}{x^2yz^3 + xyz^3 + xz^2 - 2xyz^2 - xz - z + 1}.$$

Taking the derivative w.r.t. y and setting $y = 1$ yields

$$\frac{\partial}{\partial y} G(x,y,z)\bigg|_{y=1} = \sum_{k,\ell,n\geq 0} \ell a_{k,\ell,n} x^k z^n = \frac{xz\left(x^2z^2 + xz^2 - 1\right)}{(xz + z - 1)^2\left(xz^2 - 1\right)}.$$

Dividing the coefficient of $x^k z^n$ by the number $\binom{n}{k}$ of standard binary expansions of length $\leq n$ and weight k gives the expected Hamming weight.

Idea of the Proof (2)

$$G(x,y,z) = \sum_{k,\ell,n\geq 0} a_{k,\ell,n} x^k y^\ell z^n$$
$$= \frac{x^2y^2z^2 - x^2yz^2 - xyz^2 - xz + xyz + 1}{x^2yz^3 + xyz^3 + xz^2 - 2xyz^2 - xz - z + 1}.$$

Taking the derivative w.r.t. y and setting $y = 1$ yields

$$\frac{\partial}{\partial y} G(x,y,z)\bigg|_{y=1} = \sum_{k,\ell,n\geq 0} \ell a_{k,\ell,n} x^k z^n = \frac{xz\left(x^2z^2 + xz^2 - 1\right)}{(xz + z - 1)^2\left(xz^2 - 1\right)}.$$

Dividing the coefficient of $x^k z^n$ by the number $\binom{n}{k}$ of standard binary expansions of length $\leq n$ and weight k gives the expected Hamming weight.

Using methods of multivariate asymptotics gives the result: Bender and Richmond's method is used.

Fixed Input Weight

Other point of view: fixed input Hamming weight, length $n \to \infty$.

Fixed Input Weight

Other point of view: fixed input Hamming weight, length $n \to \infty$.

Theorem

Let k be a fixed integer. Then the expected Hamming weight of the NAF of an integer with standard binary digit expansion of Hamming weight k and length $\leq n$ is asymptotically

$$k - \frac{k(k^2 - 3k + 2)}{n^2} + O\left(\frac{1}{n^3} + \frac{1}{n^{k-1}}\right),$$

Fixed Input Weight

Other point of view: fixed input Hamming weight, length $n \to \infty$.

Theorem

Let k be a fixed integer. Then the expected Hamming weight of the NAF of an integer with standard binary digit expansion of Hamming weight k and length $\leq n$ is asymptotically

$$k - \frac{k(k^2 - 3k + 2)}{n^2} + O\left(\frac{1}{n^3} + \frac{1}{n^{k-1}}\right),$$

whereas the expected Hamming weight of the NAF of an integer with standard binary digit expansion of Hamming weight $(n-k)$ and length $\leq n$ is asymptotically

$$(k+2) - \frac{2k}{n} - \frac{(k-1)k(k+2)}{n^2} + O\left(\frac{1}{n^3} + \frac{1}{n^{k-1}}\right).$$

Comments

Fixed input weight k:

$$k - \frac{k(k^2 - 3k + 2)}{n^2} + O\left(\frac{1}{n^3} + \frac{1}{n^{k-1}}\right),$$

i.e., the main term corresponds to just keeping the input expansion untouched.

Comments

Fixed input weight k:

$$k - \frac{k(k^2 - 3k + 2)}{n^2} + O\left(\frac{1}{n^3} + \frac{1}{n^{k-1}}\right),$$

i.e., the main term corresponds to just keeping the input expansion untouched.

Fixed input weight $n - k$:

$$(k+2) - \frac{2k}{n} - \frac{(k-1)k(k+2)}{n^2} + O\left(\frac{1}{n^3} + \frac{1}{n^{k-1}}\right),$$

i.e., the main term corresponds passing to the one's complement and two additional repairing operations.

Large Input Weight

Theorem

The expected Hamming weight of the NAF of an integer with unsigned binary expansion of length $\leq n$ *and weight* $\geq n/2$ *equals*

$$\frac{n}{3} + \frac{4}{9} + \frac{2\sqrt{2}\,(7 + (-1)^n)}{9\pi} \cdot \frac{1}{\sqrt{n}} - \frac{16\,(1 + (-1)^n)}{9\pi} \cdot \frac{1}{n} + O\left(\frac{1}{n^{3/2}}\right).$$

Large Input Weight

Theorem

The expected Hamming weight of the NAF of an integer with unsigned binary expansion of length $\leq n$ and weight $\geq n/2$ equals

$$\frac{n}{3} + \frac{4}{9} + \frac{2\sqrt{2}\,(7 + (-1)^n)}{9\pi} \cdot \frac{1}{\sqrt{n}} - \frac{16\,(1 + (-1)^n)}{9\pi} \cdot \frac{1}{n} + O\left(\frac{1}{n^{3/2}}\right).$$

The expected Hamming weight of the NAF of an integer with unsigned binary expansion of length $\leq n$ and weight $\leq n/2$ equals

$$\frac{n}{3} - \frac{(1 + (-1)^n)\sqrt{2}}{3\sqrt{\pi}}\sqrt{n} + \frac{4}{9} + \frac{2 + 2(-1)^n}{3\pi} - \frac{8 + 8(-1)^n + 23\pi + 7(-1)^n\pi}{6\sqrt{2}\sqrt{n}\pi^{3/2}} + O\left(\frac{1}{n}\right).$$

Idea of the Proof

Apply MacMahon's Ω-operator.

Idea of the Proof

Apply MacMahon's Ω-operator. Consider

$$\frac{\partial}{\partial y} G(\lambda^2, 1, z/\lambda)\Big|_{y=1} = \sum_{k,n\geq 0} b_{kn}\lambda^{2k-n} z^n$$

$$= \frac{\lambda^3 z(\lambda^2 z^2 + z^2 - 1)}{(z-1)(z+1)(z\lambda^2 - \lambda + z)^2}.$$

Idea of the Proof

Apply MacMahon's Ω-operator. Consider

$$\frac{\partial}{\partial y} G(\lambda^2, 1, z/\lambda)\bigg|_{y=1} = \sum_{k,n\geq 0} b_{kn}\lambda^{2k-n}z^n = \frac{\lambda^3 z(\lambda^2 z^2 + z^2 - 1)}{(z-1)(z+1)(z\lambda^2 - \lambda + z)^2}.$$

We are interested in the cases with $2k - n \geq 0$.

Idea of the Proof

Apply MacMahon's Ω-operator. Consider

$$\frac{\partial}{\partial y} G(\lambda^2, 1, z/\lambda)\Big|_{y=1} = \sum_{k,n\geq 0} b_{kn}\lambda^{2k-n}z^n$$

$$= \frac{\lambda^3 z(\lambda^2 z^2 + z^2 - 1)}{(z-1)(z+1)(z\lambda^2 - \lambda + z)^2}.$$

We are interested in the cases with $2k - n \geq 0$. Thus all negative powers of λ have to be eliminated by looking at the partial fraction decomposition.

Idea of the Proof

Apply MacMahon's Ω-operator. Consider

$$\frac{\partial}{\partial y} G(\lambda^2, 1, z/\lambda)\bigg|_{y=1} = \sum_{k,n\geq 0} b_{kn}\lambda^{2k-n}z^n$$

$$= \frac{\lambda^3 z(\lambda^2 z^2 + z^2 - 1)}{(z-1)(z+1)(z\lambda^2 - \lambda + z)^2}.$$

We are interested in the cases with $2k - n \geq 0$. Thus all negative powers of λ have to be eliminated by looking at the partial fraction decomposition. Afterwards, we set $\lambda = 1$ and extract the coefficient of z^n.

Idea of the Proof — Partial Fraction Decomposition

$$
\begin{aligned}
G_y(\lambda^2, 1, z/\lambda) = & \frac{\lambda z + 2}{(z-1)(z+1)} \\
& + \frac{16z^6 - 24wz^4 - 40z^4 + 13wz^2 + 17z^2 - 2w - 2}{(z-1)(z+1)(2z-1)^2(2z+1)^2(w - 2\lambda z + 1)} \\
& - \frac{2\left(2z^2 - w - 1\right) z^2}{(z-1)(z+1)(2z-1)(2z+1)(w - 2\lambda z + 1)^2} \\
& - \frac{16z^6 + 24wz^4 - 40z^4 - 13wz^2 + 17z^2 + 2w - 2}{(z-1)(z+1)(2z-1)^2(2z+1)^2(w + 2\lambda z - 1)} \\
& - \frac{2\left(2z^2 + w - 1\right) z^2}{(z-1)(z+1)(2z-1)(2z+1)(w + 2\lambda z - 1)^2},
\end{aligned}
$$

where the abbreviation $w := \sqrt{1 - 4z^2}$ has been used.

Applying MacMahon's Operator

We have

$$\frac{1}{w-2\lambda z+1}=\frac{1}{(1+w)\left(1-\frac{2\lambda z}{1+w}\right)}=\sum_{m\geq 0}\frac{(2\lambda z)^m}{(1+w)^{m+1}},$$

keeping in mind that

$$\frac{2\lambda z}{1+w}\sim z,$$

for $z\to 0$ and $\lambda\to 1$, thus the former survives MacMahon's Ω

Applying MacMahon's Operator

We have

$$\frac{1}{w-2\lambda z+1}=\frac{1}{(1+w)\left(1-\frac{2\lambda z}{1+w}\right)}=\sum_{m\geq 0}\frac{(2\lambda z)^m}{(1+w)^{m+1}},$$

$$\frac{1}{w+2\lambda z-1}=\frac{1}{2\lambda z\left(1-\frac{1-w}{2\lambda z}\right)}=\sum_{m\geq 0}\frac{(1-w)^m}{(2\lambda z)^{m+1}},$$

keeping in mind that

$$\frac{2\lambda z}{1+w}\sim z, \qquad \frac{1-w}{2\lambda z}\sim\frac{2z^2}{2z}=z$$

for $z\to 0$ and $\lambda\to 1$, thus the former survives MacMahon's Ω, while the latter does not.

Applying MacMahon's Operator

We have

$$\frac{1}{w-2\lambda z+1}=\frac{1}{(1+w)\left(1-\frac{2\lambda z}{1+w}\right)}=\sum_{m\geq 0}\frac{(2\lambda z)^m}{(1+w)^{m+1}},$$

$$\frac{1}{w+2\lambda z-1}=\frac{1}{2\lambda z\left(1-\frac{1-w}{2\lambda z}\right)}=\sum_{m\geq 0}\frac{(1-w)^m}{(2\lambda z)^{m+1}},$$

keeping in mind that

$$\frac{2\lambda z}{1+w}\sim z,\qquad \frac{1-w}{2\lambda z}\sim\frac{2z^2}{2z}=z$$

for $z\to 0$ and $\lambda\to 1$, thus the former survives MacMahon's Ω, while the latter does not. Singularity analysis does the rest.

Binary and NAF Weight As a Random Vector

Up to now, we always had the input weight k as a parameter.

Binary and NAF Weight As a Random Vector

Up to now, we always had the input weight k as a parameter.
Now: n is the only parameter. Study the random variables $H(\mathrm{Binary}(X_n))$ and $H(\mathrm{NAF}(X_n))$, where

Binary and NAF Weight As a Random Vector

Up to now, we always had the input weight k as a parameter. Now: n is the only parameter. Study the random variables $H(\mathrm{Binary}(X_n))$ and $H(\mathrm{NAF}(X_n))$, where

- X_n ... random nonnegative integer with standard binary expansion of length $\leq n$,

Binary and NAF Weight As a Random Vector

Up to now, we always had the input weight k as a parameter. Now: n is the only parameter. Study the random variables $H(\mathrm{Binary}(X_n))$ and $H(\mathrm{NAF}(X_n))$, where

- X_n ... random nonnegative integer with standard binary expansion of length $\leq n$,
- $\mathrm{Binary}(m)$ ... standard binary expansion of m,

Binary and NAF Weight As a Random Vector

Up to now, we always had the input weight k as a parameter. Now: n is the only parameter. Study the random variables $H(\mathrm{Binary}(X_n))$ and $H(\mathrm{NAF}(X_n))$, where

- X_n ... random nonnegative integer with standard binary expansion of length $\leq n$,
- $\mathrm{Binary}(m)$ ... standard binary expansion of m,
- $\mathrm{NAF}(m)$ ... NAF of m,

Binary and NAF Weight As a Random Vector

Up to now, we always had the input weight k as a parameter. Now: n is the only parameter. Study the random variables $H(\mathrm{Binary}(X_n))$ and $H(\mathrm{NAF}(X_n))$, where

- X_n ... random nonnegative integer with standard binary expansion of length $\leq n$,
- $\mathrm{Binary}(m)$ ... standard binary expansion of m,
- $\mathrm{NAF}(m)$ ... NAF of m,
- $H(\cdot)$ ... Hamming weight of an expansion.

Covariance

Theorem

We have

$$\begin{aligned}
\mathbb{E}(H(\mathrm{Binary}(X_n))) &= \frac{n}{2},\\
\mathbb{E}(H(\mathrm{NAF}(X_n))) &= \frac{n}{3} + \frac{4}{9} + O(2^{-n}),\\
\mathrm{Var}(H(\mathrm{Binary}(X_n))) &= \frac{n}{4},\\
\mathrm{Var}(H(\mathrm{NAF}(X_n))) &= \frac{2n}{27} + \frac{14}{81} + O(n2^{-n}),\\
\mathrm{Cov}(H(\mathrm{Binary}(X_n)), H(\mathrm{NAF}(X_n))) &= \frac{2}{3} + O(n2^{-n}).
\end{aligned}$$

Limiting Distribution

Theorem

The random vector $\mathbf{V}_n := (H(\mathrm{Binary}(X_n)), H(\mathrm{NAF}(X_n)))$ *is asymptotically normal, i.e.,*

$$\mathbb{P}\left(\frac{\mathbf{V}_n - \binom{1/2}{1/3}n}{\sqrt{n}} \le \mathbf{x}\right) = \frac{1}{54}\Phi(2x_1)\Phi\left(\frac{3\sqrt{3}}{\sqrt{2}}x_2\right) + O\left(\frac{1}{\sqrt{n}}\right),$$

where

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}\,dt.$$

Limiting Distribution

Theorem

The random vector $\mathbf{V}_n := (H(\mathrm{Binary}(X_n)), H(\mathrm{NAF}(X_n)))$ *is asymptotically normal, i.e.,*

$$\mathbb{P}\left(\frac{\mathbf{V}_n - \binom{1/2}{1/3} n}{\sqrt{n}} \le \mathbf{x}\right) = \frac{1}{54}\Phi(2x_1)\Phi\left(\frac{3\sqrt{3}}{\sqrt{2}}x_2\right) + O\left(\frac{1}{\sqrt{n}}\right),$$

where

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\, dt.$$

This means that although $H(\mathrm{Binary}(X_n))$ and $H(\mathrm{NAF}(X_n))$ are correlated, they are asymptotically independent. Their limiting distribution is the product of two normal distributions.

Limiting Distribution

Theorem

The random vector $\mathbf{V}_n := (H(\mathrm{Binary}(X_n)), H(\mathrm{NAF}(X_n)))$ *is asymptotically normal, i.e.,*

$$\mathbb{P}\left(\frac{\mathbf{V}_n - \binom{1/2}{1/3} n}{\sqrt{n}} \le \mathbf{x}\right) = \frac{1}{54}\Phi(2x_1)\Phi\left(\frac{3\sqrt{3}}{\sqrt{2}}x_2\right) + O\left(\frac{1}{\sqrt{n}}\right),$$

where

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\, dt.$$

This means that although $H(\mathrm{Binary}(X_n))$ and $H(\mathrm{NAF}(X_n))$ are correlated, they are asymptotically independent. Their limiting distribution is the product of two normal distributions. This is proved via a 2-dimensional version of Hwang's Quasi-Power Thm.

Quasi-Power Theorem, Dimension 1

Theorem (Hwang)

Let $\{\Omega_n\}_{n\geq 1}$ be a sequence of integral random variables. Suppose that the moment generating function satisfies the asymptotic expression

$$\mathbb{E}(e^{\Omega_n s}) = \sum_{m\geq 0} \mathbb{P}(\Omega_n = m) e^{ms} = e^{u(s)\phi(n)+v(s)}(1 + O(\kappa_n^{-1})),$$

the O-term being uniform for $|s| \leq \tau$, $s \in \mathbb{C}$, $\tau > 0$, where

Quasi-Power Theorem, Dimension 1

Theorem (Hwang)

Let $\{\Omega_n\}_{n\geq 1}$ be a sequence of integral random variables. Suppose that the moment generating function satisfies the asymptotic expression

$$\mathbb{E}(e^{\Omega_n s}) = \sum_{m\geq 0} \mathbb{P}(\Omega_n = m) e^{ms} = e^{u(s)\phi(n)+v(s)}(1 + O(\kappa_n^{-1})),$$

the O-term being uniform for $|s| \leq \tau$, $s \in \mathbb{C}$, $\tau > 0$, where

1. *$u(s)$ and $v(s)$ are analytic for $|s| \leq \tau$ and independent of n; and $u''(0) \neq 0$;*

Quasi-Power Theorem, Dimension 1

Theorem (Hwang)

Let $\{\Omega_n\}_{n\geq 1}$ be a sequence of integral random variables. Suppose that the moment generating function satisfies the asymptotic expression

$$\mathbb{E}(e^{\Omega_n s}) = \sum_{m\geq 0} \mathbb{P}(\Omega_n = m) e^{ms} = e^{u(s)\phi(n)+v(s)}(1 + O(\kappa_n^{-1})),$$

the O-term being uniform for $|s| \leq \tau$, $s \in \mathbb{C}$, $\tau > 0$, where

1. *$u(s)$ and $v(s)$ are analytic for $|s| \leq \tau$ and independent of n; and $u''(0) \neq 0$;*
2. $\lim_{n\to\infty} \phi(n) = \infty$;

Quasi-Power Theorem, Dimension 1

Theorem (Hwang)

Let $\{\Omega_n\}_{n\geq 1}$ be a sequence of integral random variables. Suppose that the moment generating function satisfies the asymptotic expression

$$\mathbb{E}(e^{\Omega_n s}) = \sum_{m\geq 0} \mathbb{P}(\Omega_n = m)e^{ms} = e^{u(s)\phi(n)+v(s)}(1 + O(\kappa_n^{-1})),$$

the O-term being uniform for $|s| \leq \tau$, $s \in \mathbb{C}$, $\tau > 0$, where

1. *$u(s)$ and $v(s)$ are analytic for $|s| \leq \tau$ and independent of n; and $u''(0) \neq 0$;*
2. $\lim_{n\to\infty} \phi(n) = \infty$;
3. $\lim_{n\to\infty} \kappa_n = \infty$.

Quasi-Power Theorem, Dimension 1, continued

$$\mathbb{E}(e^{\Omega_n s}) = \sum_{m\geq 0} \mathbb{P}(\Omega_n = m)e^{ms} = e^{u(s)\phi(n)+v(s)}(1 + O(\kappa_n^{-1})),$$

Quasi-Power Theorem, Dimension 1, continued

$$\mathbb{E}(e^{\Omega_n s}) = \sum_{m\geq 0} \mathbb{P}(\Omega_n = m)e^{ms} = e^{u(s)\phi(n)+v(s)}(1 + O(\kappa_n^{-1})),$$

Theorem (Hwang, cont.)

Then the distribution of Ω_n is asymptotically normal, i.e.,

$$\mathbb{P}\left(\frac{\Omega_n - u'(0)\phi(n)}{\sqrt{u''(0)\phi(n)}} < x\right) = \Phi(x) + O\left(\frac{1}{\sqrt{\phi(n)}} + \frac{1}{\kappa_n}\right),$$

uniformly with respect to x, $x \in \mathbb{R}$, where Φ denotes the standard normal distribution

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp\left(-\frac{1}{2}y^2\right)\,dy.$$

Quasi-Power Theorem, Dimension 2

Theorem

Let $\{\mathbf{\Omega}_n\}_{n\geq 1}$ be a sequence of two dimensional integral random vectors.

Quasi-Power Theorem, Dimension 2

Theorem

Let $\{\mathbf{\Omega}_n\}_{n\geq 1}$ be a sequence of two dimensional integral random vectors. Suppose that the moment generating function satisfies the asymptotic expression

$$\mathbb{E}(e^{\langle \mathbf{\Omega}_n, \mathbf{s}\rangle}) = \sum_{\mathbf{m}\geq 0} \mathbb{P}(\mathbf{\Omega}_n = \mathbf{m}) e^{\langle \mathbf{m}, \mathbf{s}\rangle} = e^{u(\mathbf{s})\phi(n)+v(\mathbf{s})}(1 + O(\kappa_n^{-1})),$$

the O-term being uniform for $\|\mathbf{s}\|_\infty \leq \tau$, $\mathbf{s} \in \mathbb{C}^2$, $\tau > 0$, where

Quasi-Power Theorem, Dimension 2

Theorem

Let $\{\mathbf{\Omega}_n\}_{n\geq 1}$ be a sequence of two dimensional integral random vectors. Suppose that the moment generating function satisfies the asymptotic expression

$$\mathbb{E}(e^{\langle \mathbf{\Omega}_n, \mathbf{s}\rangle}) = \sum_{\mathbf{m}\geq 0} \mathbb{P}(\mathbf{\Omega}_n = \mathbf{m}) e^{\langle \mathbf{m}, \mathbf{s}\rangle} = e^{u(\mathbf{s})\phi(n)+v(\mathbf{s})}(1 + O(\kappa_n^{-1})),$$

the O-term being uniform for $\|\mathbf{s}\|_\infty \leq \tau$, $\mathbf{s} \in \mathbb{C}^2$, $\tau > 0$, where

1. *$u(\mathbf{s})$ and $v(\mathbf{s})$ analytic for $\|\mathbf{s}\| \leq \tau$ and independent of n; and the Hessian $H_u(\mathbf{0})$ of u at the origin is nonsingular;*

Quasi-Power Theorem, Dimension 2

Theorem

Let $\{\mathbf{\Omega}_n\}_{n\geq 1}$ be a sequence of two dimensional integral random vectors. Suppose that the moment generating function satisfies the asymptotic expression

$$\mathbb{E}(e^{\langle \mathbf{\Omega}_n, \mathbf{s}\rangle}) = \sum_{\mathbf{m}\geq 0} \mathbb{P}(\mathbf{\Omega}_n = \mathbf{m}) e^{\langle \mathbf{m}, \mathbf{s}\rangle} = e^{u(\mathbf{s})\phi(n)+v(\mathbf{s})}(1 + O(\kappa_n^{-1})),$$

the O-term being uniform for $\|\mathbf{s}\|_\infty \leq \tau$, $\mathbf{s} \in \mathbb{C}^2$, $\tau > 0$, where

1. *$u(\mathbf{s})$ and $v(\mathbf{s})$ analytic for $\|\mathbf{s}\| \leq \tau$ and independent of n; and the Hessian $H_u(\mathbf{0})$ of u at the origin is nonsingular;*
2. $\lim_{n\to\infty} \phi(n) = \infty$*;*

Quasi-Power Theorem, Dimension 2

Theorem

Let $\{\mathbf{\Omega}_n\}_{n\geq 1}$ be a sequence of two dimensional integral random vectors. Suppose that the moment generating function satisfies the asymptotic expression

$$\mathbb{E}(e^{\langle \mathbf{\Omega}_n, \mathbf{s}\rangle}) = \sum_{\mathbf{m}\geq 0} \mathbb{P}(\mathbf{\Omega}_n = \mathbf{m}) e^{\langle \mathbf{m}, \mathbf{s}\rangle} = e^{u(\mathbf{s})\phi(n)+v(\mathbf{s})}(1+O(\kappa_n^{-1})),$$

the O-term being uniform for $\|\mathbf{s}\|_\infty \leq \tau$, $\mathbf{s}\in\mathbb{C}^2$, $\tau>0$, where

1. *$u(\mathbf{s})$ and $v(\mathbf{s})$ analytic for $\|\mathbf{s}\|\leq\tau$ and independent of n; and the Hessian $H_u(\mathbf{0})$ of u at the origin is nonsingular;*
2. $\lim_{n\to\infty}\phi(n)=\infty$;
3. $\lim_{n\to\infty}\kappa_n=\infty$.

Quasi-Power Theorem, Dimension 2, continued

$$\mathbb{E}(e^{\langle \boldsymbol{\Omega}_n, \mathbf{s} \rangle}) = e^{u(\mathbf{s})\phi(n)+v(\mathbf{s})}(1 + O(\kappa_n^{-1})),$$

Quasi-Power Theorem, Dimension 2, continued

$$\mathbb{E}(e^{\langle \mathbf{\Omega}_n, \mathbf{s}\rangle}) = e^{u(\mathbf{s})\phi(n)+v(\mathbf{s})}(1 + O(\kappa_n^{-1})),$$

Theorem (cont.)

Then, the distribution of $\mathbf{\Omega}_n$ is asymptotically normal, i.e.,

$$\mathbb{P}\left(\frac{\mathbf{\Omega}_n - \operatorname{grad} u(\mathbf{0})\phi(n)}{\sqrt{\phi(n)}} \le \mathbf{x}\right) = \Phi_{H_u(\mathbf{0})}(\mathbf{x}) + O\left(\frac{1}{\sqrt{\phi(n)}} + \frac{1}{\kappa_n}\right),$$

where Φ_Σ is the distribution function of the two dimensional normal distribution with mean $\mathbf{0}$ and variance-covariance matrix Σ:

$$\Phi_\Sigma(\mathbf{x}) = \frac{1}{2\pi\sqrt{\det\Sigma}} \iint_{\substack{y_1\le x_1\\ y_2\le x_2}} \exp\left(-\frac{1}{2}\mathbf{y}^t\Sigma^{-1}\mathbf{y}\right)\, d\mathbf{y}.$$

Lemma (Sadikova)

Let $\mathbf{X}$ *and* $\mathbf{Y}$ *be two-dimensional random vectors with distribution functions* F *and* G *and characteristic functions* f *and* g*,*

$$\hat{f}(s_1, s_2) = f(s_1, s_2) - f(s_1, 0) f(0, s_2),$$
$$\hat{g}(s_1, s_2) = g(s_1, s_2) - g(s_1, 0) g(0, s_2),$$
$$A_1 = \sup_{x_1, x_2} \frac{\partial G(x_1, x_2)}{\partial x_1}, \qquad A_2 = \sup_{x_1, x_2} \frac{\partial G(x_1, x_2)}{\partial x_2}.$$

Then for any $T > 0$*, we have*

$$\frac{1}{2} \sup_{x,y} |F(x,y) - G(x,y)| \leq \frac{1}{(2\pi)^2} \iint_{\|\mathbf{s}\| \leq T} \left| \frac{\hat{f}(s_1, s_2) - \hat{g}(s_1, s_2)}{s_1 s_2} \right| d\mathbf{s}$$
$$+ \sup_x |F(x, \infty) - G(x, \infty)| + \sup_y |F(\infty, y) - G(\infty, y)| + \frac{12(A_1 + A_2)}{T}.$$