Evaluation of a coding design for a very noisy channel

Paul Camion, J.L. Politano

INRIA

UNITE DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
BP 105
78153 Le Chesnay Cedex
France
Tél (1) 39 63 55 11

Rapports de Recherche

N° 946

Programme 1

EVALUATION OF A CODING DESIGN FOR A VERY NOISY CHANNEL

Paul CAMION
Jean-Luc POLITANO

Décembre 1988

EVALUATION OF A CODING DESIGN FOR A VERY NOISY CHANNEL

EVALUATION D'UNE CONFIGURATION DE CODAGE POUR UNE LIGNE TRES BRUITEE

Paul CAMION, CNRS et INRIA
Jean-Luc POLITANO, ATFH et INRIA

INRIA - Domaine de Voluceau - Rocquencourt - BP 105
78153 LE CHESNAY Cedex - FRANCE
ATFH - 55 rue Greffülhe - 92301 LEVALLOIS PERRET - FRANCE

ABSTRACT

An interleaving array of depth I comprises I code-words obtained by concatenating two codes. The symbols of that array are permuted according to a pseudo-random law. The sequence of symbols obtained in that way is transmitted over a very noisy channel. That channel can be for example an erasable recording medium. It is assumed that at most E erasures may occur which appear in the restored array as if they were dealt according to a uniform probability law. A random variable θ is defined over the set of all arrays comprising E erasures. The value of θ is the number of concatenated code-words in the array that may be corrected. The notion of polynomial of correctable patterns is introduced. That polynomial allows calculating the moments of the random variable θ. To set one's ideas, the investigation is lead on the particular case of concatenating a Reed-Solomon (14,7) code and a Hamming (8,4) binary code.

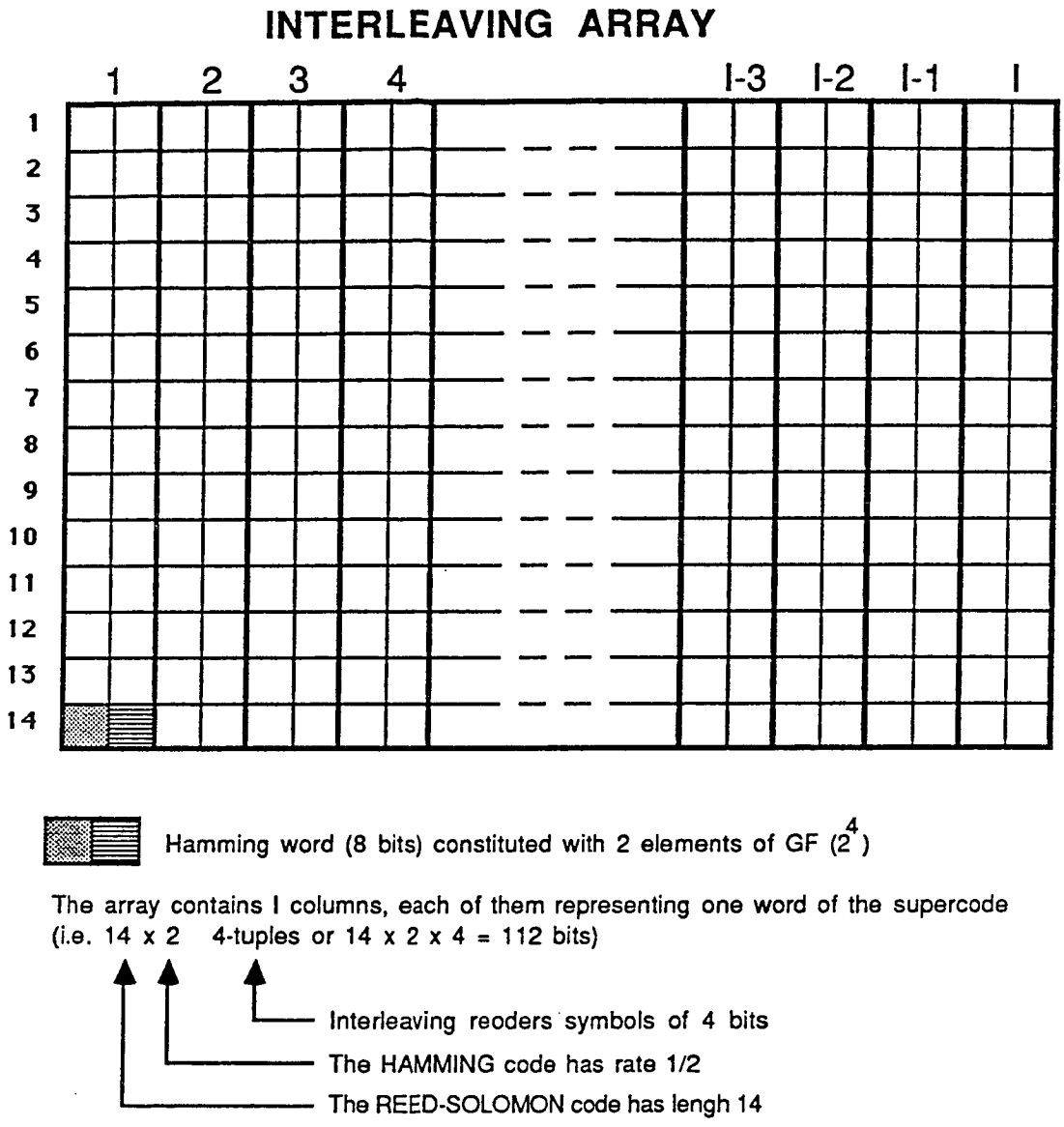
Key-words : Code, concatenation, pseudo-random interleaving, erasures, polynomial of correctable patterns.

RESUME

Un tableau d'entrelacement de profondeur I comporte I mots obtenus par concaténation de deux codes. On permute les symboles de ce tableau au moyen d'une loi pseudo-aléatoire. La suite de symboles ainsi obtenue est transmise sur une ligne très bruitée. Cette ligne peut être par exemple un support d'enregistrement effaçable. On suppose qu'il se produit au plus E effacements qui apparaissent dans le tableau reconstitué comme s'ils avaient été distribués selon une loi de probabilité uniforme. Sur l'ensemble des tableaux comportant E effacements, on définit une variable aléatoire θ dont la valeur est le nombre de mots de code concaténés corrigibles dans le tableau. La notion de polynôme des schémas corrigibles est introduite. Ce polynôme permet de calculer les moments de la variable aléatoire θ. Pour fixer les idées, l'étude est faite sur le cas particulier de la concaténation d'un Reed-Solomon (14,7) et d'un Hamming (8,4).

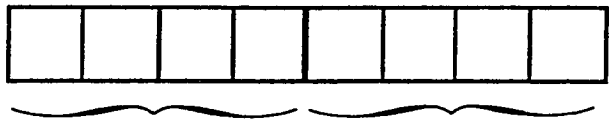
Mots-clés : Code, concaténation, entrelacement pseudo-aléatoire, effacements, polynôme des schémas corrigibles.

We consider the coding scheme based on concatenating two codes and interleaving the supercode [1] pseudo-randomly. The inner code is a binary Hamming (8,4) and the outer one is a Reed Solomon (14,7) with symbols from GF(2^4).
Interleaving reorders symbols of four bits and the array can be represented as follows.



Among the 2nI symbols (n=14), E erasures are dealt out according to a pseudo-random law. Given a rate of erasures, $r = \frac{E}{2nI}$, we want to compute the residual rate of non correctable words of the supercode (RRNCW).
In the following expressions, the power of the variable x points out the number of erased symbols in the array.
An additive white gaussian noise affects the transmitted bits. Then, we assume that we have the correct erased symbols of four bits and moreover errors for a binary symmetric channel. We assume that each transmitted bit is received in error with probability p or received correctly with probability q=1-p.

We can now define the three polynomials λ, μ and ν related to one word of the inner code that we can represent as follows :



4-tuple corresponding to a symbol of a Reed Solomon word

4-tuple of redundancy brought by the Hamming code.

The inner code succeeds in correcting a word (one byte) iff :
- No one of the two 4-tuples is erased and there is at most one bit in error in the received word.
- One of the two 4-tuples is erased the other one does not contain any bit in error.

The situation can be represented using the following polynomial :

$$\lambda = \binom{2}{1}\binom{4}{0}q^4x + \left(\binom{8}{0}q^8 + \binom{8}{1}pq^7\right) = 2q^4x + \left(q^8 + 8pq^7\right)$$

The most frequent situations where the inner code transmits a signal of detection to the outer code are :
- Both of the 4-tuples are erased.
- No one of the two 4-tuples is erased but there are two bits in error in the word.

These situations can be represented using the following polynomial :

$$\mu = \binom{2}{2}x^2 + \binom{8}{2}p^2q^6 = x^2 + 28\,p^2q^6$$

The inner code transmits an erroneous symbol to the outer code in most others cases. The set of situations complementary to the one described by $\lambda+\mu$ can be represented by the polynomial :

$$\nu = 2x(1-q^4) + (1-q^8 - 8pq^7 - 28\,p^2q^6)$$

One word of the inner code is constructed with two 4-tuples, each of them beeing or not an erasure represented by the power of the variable x. We have that $\lambda+\mu+\nu = (1+x)^2$, polynomial of which each term corresponds to one of the four situations for two quadruples forming a Hamming codeword regarding erasures.

We define the polynomial f(x) of correctable patterns. A Reed-Solomon word code can be corrected iff :
2 x (number of symbols in error) + (number of erased symbols) < d-1 where d is the minimum distance of the Reed-Solomon code and is : 14-7+1 = 8.

$$f(x) = \sum_{a=0}^{d-1} \binom{n}{a} \mu^a \sum_{b=0}^{\left\lfloor \frac{d-1-a}{2} \right\rfloor} \binom{n-a}{b} \nu^b \lambda^{n-a-b} = \sum_{i=0}^{n+d-1} f_i x^i$$

There are $\binom{2n}{i}$ ways to put i erasures in one column (i.e. one concatenated word).

When a column contains i erasures, the probability to correct this code word equals $\frac{f_i}{\binom{2n}{i}}$.

Let T be the set of interleaving schemes such that exactly E symbols among the 2nI of the array are erased.

Then $|T| = \binom{2nI}{E}$

We introduce a random variable θ defined on T and wich takes values in [0,I] such that :

$$\forall u = (u_1, u_2, \ldots, u_I) \in T, \theta(u) = |\{j/j \text{ is correctable}\}|$$

The residual rate of non correctable words of concatenated codes equals RRNCW = $1-\frac{\bar{\theta}}{I}$

with $\bar{\theta} = \sum_{s=0}^{I} s \text{ prob } \{\theta=s\}$

In fact, we shall see that this polynomial of correctable patterns f(x) allows calculating the different moments of the variable θ.

We denote by $g(x) = \sum_{i=0}^{2n} \binom{2n}{i} x^i = (1+x)^{2n}$ the polynomial of all the different patterns for one column (i.e one word of supercode). Then g(x)-f(x) is the polynomial of non correctable patterns.

$$\text{Prob } \{\theta=s\} = |T|^{-1} \left[x^E\right] \binom{I}{s} (f(x))^s (g(x)-f(x))^{I-s}$$

Prob $\{\theta=s\}$ is the conditional probability that s columns among the I ones of the interleaving array will be correctable, relative to the hypothesis that E erasures occured in the interleaving array.

To compute $\bar{\theta}$, we use the polynomial $\varphi(z)$ defined as :

$$\varphi(z) = \sum_{s=0}^{I} \text{Prob } \{\theta = s\} \, z^s$$

Therefore we have that $\bar{\theta} = \frac{d}{dz}\,\varphi(z)\Big|_{z=1}$

$$\varphi(z) = |T|^{-1}[x^E] \sum_{s=0}^{I} \binom{I}{s} (f(x))^s\,(g(x)-f(x))^{I-s}\,z^s$$

$$\varphi(z) = |T|^{-1}[x^E]\,(g(x)+(z-1)\,f(x))^I$$

$$\bar{\theta} = \frac{d}{dz}\,\varphi(z)\Big|_{z=1} = |T|^{-1}[x^E] I\,(g(x)+(z-1)f(x))^{I-1}\,f(x)\Big|_{z=1}$$

$$\bar{\theta} = |T|^{-1}[x^E]\,I\,(g(x))^{I-1}\,f(x)$$

$$(g(x))^{I-1} = (1+x)^{2n\,(I-1)} = \sum_{i=0}^{n+d-1} \binom{2n(I-1)}{i} x^i$$

$$\bar{\theta} = |T|^{-1}\,I \sum_{i=0}^{n+d-1} f_i \binom{2n(I-1)}{E-i}$$

Here, the residual rate of non correctable words equals :

$$RRNCW = 1-\frac{\bar{\theta}}{I} = 1 - \sum_{i=0}^{n+d-1} f_i \frac{\binom{2n(I-1)}{E-i}}{\binom{2nI}{E}}$$

Remarks :

- We get the result that we would have found using the hypergeometric distribution [2]. Let $N = 2nI$ a set of elements, $N_1 = E$ from them are erased and $N-N_1 = 2nI-E$ are not erased. A group of $R=2n$ elements is chosen at random. We seek the probability q_i that the group, so chosen will contain exactly i erased elements.

$$q_i = \frac{\binom{N_1}{i}\binom{N-N_1}{R-i}}{\binom{N}{R}} = \frac{\binom{R}{i}\binom{N-R}{N_1-i}}{\binom{N}{N_1}}$$

The system of probabilities so defined is called the hypergeometric distribution.
In the case under consideration, we may compute :

$$RRNCW_{\text{hypergeometric}} = 1 - \sum_{i=0}^{n+d-1} \text{Prob}\,\{i\}.\ \text{Prob}\,\{\text{correction} / i\}.$$

Here Prob {i} is the probability that the 2n 4-tuples, constituting a word of the supercode, will contain exactly i erased symbols and Prob {correction / i} is the conditional probability that a column will be correctable relative to the hypothesis that i erasures occured in this word.

$$RRNCW_{\text{hypergeometric}} = 1 - \sum_{i=0}^{n+d-1} q_i \frac{f_i}{\binom{2n}{i}} = 1 - \sum_{i=0}^{n+d-1} \frac{\binom{2n}{i}\binom{2nI-2n}{E-i}}{\binom{2n}{i}\binom{2nI}{E}} f_i = RRNCW$$

- As the interleaving depth I becomes arbitrarily large and for a constant rate of erasures $r = \frac{E}{2nI}$, we show that erasures occur according to a Bernoulli's law.

Proof :

$$\frac{\binom{2nI-2n}{E-i}}{\binom{2nI}{E}} = \frac{(2nI-2n)!}{(2nI)!} \frac{E!}{(E-i)!} \frac{(2nI-E)!}{(2nI-E-2n+i)!}$$

Using the Stirling's formula : $\lim_{a\to\infty} a! = \sqrt{2\pi}\, e^{-a}\, a^{a+1/2}\left(1 + \frac{1}{12a} + o\left(\frac{1}{a^2}\right)\right)$

$$\lim_{I\to\infty} \frac{(2nI-2n)!}{(2nI)!} = \frac{\sqrt{2\pi}\, e^{-(2nI-2n)}}{\sqrt{2\pi}\, e^{-2nI}} \frac{(2nI-2n)^{2nI-2n+1/2}}{(2nI)^{2nI+1/2}} \frac{1+\frac{1}{12(2nI-2n)}}{1+\frac{1}{12(2nI)}}$$

As I grows to infinity we can write :

$$\lim_{I\to\infty} \frac{(2nI-2n)^{2nI-2n+1/2}}{(2nI)^{2nI+1/2}} = (2nI)^{-2n}\, e^{-2n} \left(1+\frac{2n-1}{2I} + o\left(\frac{1}{I^2}\right)\right)$$

$$\text{and } \lim_{I\to\infty} \frac{1+\frac{1}{12(2nI-2n)}}{1+\frac{1}{12(2nI)}} = 1 + o\left(\frac{1}{I^2}\right)$$

$$\text{Therefore } \lim_{I\to\infty} \frac{(2nI-2n)!}{(2nI)!} = (2nI)^{-2n} \left(1+\frac{2n-1}{2I} + o\left(\frac{1}{I^2}\right)\right)$$

we can show in the same way that :

$$\lim_{E\to\infty} \frac{E!}{(E-i)!} = E^i \left(1 - \frac{i^2-i}{2E} + o\left(\frac{1}{E^2}\right)\right)$$

$$\text{and } \lim_{(2nI-E)\to\infty} \frac{(2nI-E)!}{(2nI-E-2n+i)!} = (2nI-E)^{2n-i} \left(1 - \frac{(2n-i)^2-(2n-i)}{2(2nI-E)} + o\left(\frac{1}{(2nI-E)^2}\right)\right)$$

Substituting (2nIr) for E and only keeping the first order terms we just have :

$$\lim_{I\to\infty} \frac{\binom{2nI-2n}{E-i}}{\binom{2nI}{E}} = (2nI)^{-2n}\left(1+\frac{2n-1}{2I}\right)(2nIr)^{i}\left(1-\frac{i^2-i}{4nIr}\right)(2nI(1-r))^{2n-i}\left(1-\frac{(2n-i)^2-(2n-i)}{4nI(1-r)}\right)$$

Hence,

$$\lim_{I\to\infty} \frac{\binom{2nI-2n}{E-i}}{\binom{2nI}{E}} = \left(\frac{2nIr}{2nI}\right)^{i}\left(\frac{2nI(1-r)}{2nI}\right)^{2n-i}\left(1+\frac{1}{I}\,\frac{(2n-4n^2)r^2+(4in-2i)r-i^2+i}{4n\,r\,(1-r)}\right)$$

$$= (r)^{i}\,(1-r)^{2n-i}\left(1+\frac{1}{I}\alpha(i,n,r)\right)$$

Conclusion :

$$\lim_{I\to\infty} = 1 - \sum_{i=0}^{n+d-1} f_i\,(r)^{i}\,(1-r)^{2n-i}$$

$$= 1 - \sum_{i=0}^{n+d-1} \frac{f_i}{\binom{2n}{i}}\binom{2n}{i}(r)^{i}\,(1-r)^{2n-i} = \text{RRNCW}_{\text{Bernoulli}}$$

As I grows to infinity, each symbol has a probability $r = \frac{E}{2nI}$ to be erased.

The method suggested to compute $\bar{\theta}$ also allows defining and computing the other moments of θ. For example :

$$\overline{\theta^2} = \sum_{s=0}^{I} s^2 \;\text{Prob}\,\{\theta=s\}$$

To compute this 2nd order moment, we use the polynomial $\varphi(z)$:

$$\varphi(z) = \sum_{s=0}^{I} \text{Prob}\,\{\theta = s\}\, z^s$$

$$\frac{d^2}{dz^2}\varphi(z)\Big|_{z=1} = \sum_{s=0}^{I} (s^2-s)\,\text{Prob}\,\{\theta=s\} = \overline{\theta^2} - \bar{\theta}$$

$$\varphi(z) = |T|^{-1}[x^E] \sum_{s=0}^{I} \binom{I}{s} (f(x))^s\,(g(x)-f(x))^{I-s}\,z^s$$

$$\varphi(z) = |T|^{-1}[x^E]\,(g(x)+(z-1)\,f(x))^I$$

Therefore

$$\overline{\theta^2} = \bar{\theta} + \frac{d^2}{dz^2}\varphi(z)\Big|_{z=1} = \bar{\theta} + |T|^{-1}[x^E]I(I-1)(g(x)+(z-1)f(x))^{I-2}(f(x))2\Big|_{z=1}$$

$$\overline{\theta^2} = \bar{\theta} + |T|^{-1}[x^E]I(I-1)(g(x))^{I-2}(f(x))^2$$

Let $(f(x))^2 = \sum_{i=0}^{2(n+d-1)} (f^2)_i\, x^i$

$$(g(x))^{I-2} = (1+x)^{2n(I-2)} = \sum_{i=0}^{2n(I-2)} \binom{2n(I-2)}{i} x^i$$

Hence,

$$\overline{\theta^2} = \bar{\theta} + |T|^{-1}[x^E]I(I-1) \sum_{i=0}^{2(n+d-1)} (f^2)_i \binom{2n\,(I-2)}{E-i}$$

We easily compute the standard deviation of θ.

$\sigma_\theta = \sqrt{\overline{\theta^2} - \bar{\theta}^2}$ and use the Tschebyscheff inequality.

$$\text{Prob}\,[|\theta-\bar{\theta}| \geq \Delta] \leq \frac{\overline{\theta^2} - \bar{\theta}^2}{\Delta^2}$$

that can also be written in the form : $\text{Prob}\,[|\theta-\bar{\theta}| \leq \Delta] \geq 1 - \dfrac{\overline{\theta^2} - \bar{\theta}^2}{\Delta^2}$

Computation results :

$\text{RRNCW} = 1 - \dfrac{\bar{\theta}}{I}$ $\quad$ $\text{rate} = \dfrac{E}{2nI}$ $\quad$ $n = 14$ $\quad$ $p = 0$ $\quad$ $q = 1$

depth / rate		2	10	50	100	500	Bernoulli
3.6%	$\bar{\theta}$	2	10	49.99	99.99	499.99	2.09E-20
	RRNCW	0	0	1.54E-21	6.15E-21	1.65E-20	
	σ_θ	0	0	2.78E-10	7.85E-10	2.88E-9	
12.5%	$\bar{\theta}$	2	9.99	49.99	99.99	499.99	9.81E-12
	RRNCW	0	2.69E-13	5.34E-12	7.28E-12	9.25E-12	
	σ_θ	0	1.64E-6	1.63E-5	2.70E-5	6.80E-5	
25%	$\bar{\theta}$	2	9.99	49.99	99.99	499.99	4.97E-7
	RRNCW	0	1.35E-7	3.91E-7	4.41E-7	4.85E-7	
	σ_θ	0	1.16E-3	4.42E-3	6.64E-3	.....	

$RRNCW = 1 - \frac{\bar{\theta}}{I}$ rate $= \frac{E}{2nI}$ n = 14 p = 1.0 E-3 q = 9.99 E-1

depth / rate		2	10	50	100	500	Bernoulli
3.6%	$\bar{\theta}$	1.99	9.99	49.99	99.99	499.99	6.43E-12
	RRNCW	8.83E-19	3.18E-12	5.62E-12	6.01E-12	6.35E-12	
	σ_θ	1.33E-9	5.64E-6	1.68E-5	2.45E-5	5.63E-5	
12.5%	$\bar{\theta}$	1.99	9.99	49.99	99.99	499.99	5.67E-9
	RRNCW	3.49E-10	3.02E-9	4.98E-9	5.32E-9	5.60E-9	
	σ_θ	2.64E-5	1.74E-4	4.99E-4	7.29E-4	1.67E-3	
25.0%	$\bar{\theta}$	1.99	9.99	49.99	99.99	499.99	3.14E-6
	RRNCW	1.53E-7	1.69E-6	2.78E-6	2.95E-6	3.10E-6	
	σ_θ	5.53E-4	4.12E-3	1.18E-2	1.72E-2	.....	

Conclusions :

- According to the results, we notice that a small interleaving depth (≤ 10) is more worthwhile, at least for this coding scheme.

But in fact, I will depend on several parameters. Let r be the rate of erasures, let ℓ be the maximum length of a burst of erasures and D be the bit rate on the transmission channel. We must choose I such that :

$$\frac{D\ell}{r} \leq 2nI.4 \Rightarrow I \geq \frac{D\ell}{8nr}$$

For D = 1 Mb/s, ℓ = 1 ms and $r = \frac{1}{4}$ we find $I \geq 38$

If p = 0 RRNCW ~ 3.0 E-7
If p = 1.0 E-3 RRNCW ~ 2.0 E-6

- This method for computing the different moments of θ can be used with all coding schemes with a pseudo-random interleaving. When the polynomial of correctable patterns f(x) is computed, the formulas giving the moments of θ are still valid.

- To illustrate this, we give an example of computation for p = 0, I = 100 and $r = \frac{1}{4}$.

```
This is Macsyma 303
(c) 1976,1983, Massachusetts Institute of Technology.
All Rights Reserved.
Enhancements (c) 1983, Symbolics, Inc. All Rights Reserved.
Type trade_secret(); to see Trade Secret notice.

p:0$

taux:14/56$

kill(som)$

fpprec:50$

n:14$  d:8$

i:100$

q:1-p$

e:2*n*i*taux$

lambda:(2*x*q^4)+(q^8+8*p*q^7)$

mu:x^2+(28*p^2*q^6)$

nu:(1+x)^2-lambda-mu$

if nu=0 then (for a:0 thru (d-1) do (som[a]:lambda^(n-a)))
        else (for a:0 thru (d-1) do (som[a]:sum(binomial(n-a,b)*(nu^b)*
             (lambda^(n-a-b)),b,0,fix((d-1-a)/2))))$

polschcor:sum(som[a]*binomial(n,a)*(mu^a),a,0,(d-1))$

polschcor:expand(polschcor)$

display(polschcor)$

                    21            20            19            18            17
polschcor = 439296 x   + 2306304 x   + 6406400 x   + 12940928 x   + 21438144 x

             16            15            14            13            12
 + 30418752 x   + 37442160 x   + 40116600 x   + 37442160 x   + 30421755 x

             11            10           9           8           7
 + 21474180 x   + 13123110 x   + 6906900 x  + 3108105 x  + 1184040 x

           6          5          4         3       2
 + 376740 x  + 98280 x  + 20475 x  + 3276 x  + 378 x  + 28 x + 1

tetamoyen:sum(coeff(polschcor,x,j)*binomial(2*n*(i-1),e-j),j,0,
              hipow(polschcor,x))*i/binomial(2*n*i,e)$

disp(float(tetamoyen))$

                                 99.999955

trmnc:1-tetamoyen/i$

disp(float(trmnc))$

                                 4.414321e-07

bernoulli:1-sum(coeff(polschcor,x,j)*(taux^j)*((1-taux)^(2*n-j)),j,0,hipow(polschcor,x))$
```

```
disp(float(bernoulli))$

                                4.9652282e-07

if trmnc=0 then  disp("ecart relatif infini")
          else (ecartrelatif:(bernoulli-trmnc)/trmnc , disp(float(ecartrelatif)))$

                                0.12479998

polschcor2:polschcor↑2$

polschcor2:expand(polschcor2)$

teta2moyen:sum(coeff(polschcor2,x,j)*binomial(2*n*(i-2),e-j),j,0,
          hipow(polschcor2,x))*i*(i-1)/binomial(2*n*i,e)+tetamoyen$

disp(float(teta2moyen))$

                                9999.991

ecarttype:sqrt(teta2moyen-tetamoyen↑2)$

disp(float(bfloat(ecarttype)))$

                                6.6440012e-03
```

REFERENCES

[1] F.J. MACWILLIAMS, N.J.A. SLOANE, "The Theory of Error-Correcting Codes", North-Holland.

[2] W. FELLER, "An Introduction to Probability Theory and Its Applications", Vol. 1, Third Edition, John Wiley & Sons.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique