Multinomial Computation and Factorial Theorems for Cryptographic Algorithm and Machine Learning

Chinnaraji Annamalai
School of Management, Indian Institute of Technology, Kharagpur, India
Email: anna@iitkgp.ac.in
https://orcid.org/0000-0002-0992-2584

Abstract: Computing and combinatorial techniques with factorial and multinomial computation are used as algorithms for the programs development to apply in artificial intelligence and cybersecurity. Methodological advances in combinatorics and mathematics play a vital role in machine learning and cryptology for data analysis and artificial intelligence-based cybersecurity for protection of the computing systems, devices, networks, programs and data from cyber-attacks. In connection with these ideas, this article is prepared for applications in computing science and cybersecurity. This paper presents computing and combinatorial formulae such as theorems on factorials, binomial coefficients, multinomial computation and probability and binomial distributions.

MSC Classifications Codes: 05A10

Keywords: algorithm, combinatorics, computation, multinomial

1. Introduction

Binomial and probability distribution and combinatorial techniques are used as powerful tools in artificial intelligence and machine learning for data analysis and cybersecurity for protection of the computing systems, devices, networks, programs and data from cyber-attacks. Also, the nonnegative integers play a crucial role in factorial functions or factorials [1-5] for building the theorems that are used for algorithms and software development. The results of factorials, binomial coefficients, and multinomial computations are used as strong applications without any vulnerability in artificial intelligence and cybersecurity. These methodological advances can enable the scientific researchers to solve the most real life problems.

There are traditional binomial coefficient and optimized binomial coefficients. The techniques based on the binomial coefficients play a vital role in computing and computational science. $nC_r = \frac{n!}{r!(n-r)!}$ *and* $V_r^n = \prod_{i=1}^{r} \frac{(n+i)}{r!}$ are traditional and optimized coefficients respectively.

The comparison between traditional and optimized coefficients is given below:
$V_x^y = V_y^x$ is the otimized combination. Let $z = x + y$. Then, $zC_x = zC_y, (x, y, z \in N)$.
For example,

$$V_3^5 = V_5^3 = (5+3)C_3 = (5+3)C_5 = 56.$$

Also, $V_n^0 = V_0^n = nC_0 = nC_n = \frac{n!}{n!\,0!} = 1$ *and* $V_0^0 = 0C_0 = \frac{0!}{0!} = 1 (\because 0! = 1)$.

2. Factorial and Multinomial Computation

Combinatorics, cryptography, graph theory, discrete mathematics, computational complexity, theory of computation and automata, and data structures and algorithms are used as powerful applications in computer science and engineering including artificial intelligence, machine learning, communication and cybersecurity. In this article, multinomial computation and factorial theorems [6-15] are introduced and the relationship between factorials and integers are analyzed for further developments in combinatorics.

Thorem 2.1: For any integers p and q such that $q \geq p \geq 0$,

the divisions of factorials , that is , $\frac{q!}{p!}; \frac{(p+q)!}{p!}; \frac{(p+q)!}{q!}$ and $\frac{(p+q)}{p!\,q!}$, are integers.

Proof 1. We can prove this theorem by binomial coefficient.

The binomial coefficient is $\binom{q}{p} = \frac{q!}{p!\,(q-p)!}$. If $q = p$, then $\binom{p}{p} = \frac{p!}{p!\,(p-p)!} = 1$.

$If\ q > p, \binom{q}{p} = \frac{q!}{p!\,(q-p)!} > 1$ is an integer. $For\ example, \binom{3}{2} = \frac{3!}{2!\,1!} = 3$.

The binomial coeffi*cient* $\binom{p+q}{p} = \frac{(p+q)!}{p!\,q!} = l$ is an integer, $(l \geq 0)$.

Note that $\frac{(p+q)!}{p!\,q!} = l \implies (p+q)! = l \times p! \times q!$.

Proof 2. We can also prove this theorem by factorials with nonnegative integers.

$0! = 1;\ 1! = 1;\ 2! = 1 \times 2 = 2;\ 3! = 1 \times 2 \times 3 = 6;\ \cdots;\ p!$ for $p \geq 0$ are integers.

If $q = p \geq 0$, then $q! = p! \geq 1$. If $q > p$, $q! = p! \times (p+1)(p+2)(p+3)\cdots(q-2)(q-1)q$.

$\frac{q!}{p!} = (p+1)(p+2)(p+3)\cdots(q-2)(q-1)q$ is an integer. $As\ \frac{q!}{p!}$ is an integer,

$\frac{(p+q)!}{p!}\ and\ \frac{(p+q)!}{q!}$ are integers. Let us prove that $\frac{(p+q)!}{p!\,q!}\ is$ an integer.

$\frac{(p+q)!}{p!\,q!} = \frac{(p+1)(p+2)(p+3)\cdots(p+q)}{q!}$. Let $p = 0$. Then, $\frac{(p+1)(p+2)\cdots(p+q)}{q!} = 1$

and let $p = 1$. $\frac{2 \times 3 \times 4 \times \cdots \times q(q+1)}{q!} = \frac{q! \times (q+1)}{q!} = q+1$ is an integer, that is,

$If\ \ p \geq\ 1$, then $\frac{(p+1)(p+2)(p+3)\cdots(p+q)}{q!} \geq (q+1)$ are integers for $p = 1, 2, 3, \ldots$

$\therefore\ \ \frac{q!}{p!}; \frac{(p+q)!}{p!}; \frac{(p+q)!}{q!}$ and $\frac{(p+q)}{p!\,q!}$ are integers.

Note that $p! \leq q! \leq p!\,q! \leq (p+q)! \implies \frac{(p+q)!}{p!\,q!} \leq \frac{(p+q)!}{q!} \leq \frac{(p+q)!}{p!}$.

$Proof\ 3.\ (p+q)!\ =\ l \times \mathrm{p}! \times q!$ can be proved by mathematical induc*tion*.

Basis. Let m = 2 and n = 3. $(2+3)! = 720 = 60 \times 2! \times 3!$ is obviously true.

Inductive hypothesis. Let us assume that it is true for $(p-a)\ and\ (q-b)$,
that is, $\big((p-a)+(q-b)\big)!\ =\ \mathrm{h}\times(\mathrm{p}-\mathrm{a})!\times(q-b)!$,
where $p\geq a\geq 0$ and $q\geq b\geq 0\ \ \&\ a,b\in N$.

Inductive Step. We must show that the hypothesis is true for $(\mathrm{m}-\mathrm{b}+\mathrm{b})$ and $(n-c+c)$.
$\big((p-a+a)+(q-b+b)\big)!=h\times(p-a+a)!\ \times(q-b+b)!;\ \ (h\geq 0\ \ \&\ \ h\in N)$,
Where $N=\ \{0,1,2,2,\ \ \cdots\cdots,\}$ is a set of natural numbers including zero.

By simplifying this result, we get $(p+q)!=\ l\times \mathrm{p}!\times q!;\ (h=l\geq 0\ \&\ \ l\in N)$.
Hence, theorem is proved.

Theorem 2.2 : For any k nonnegative integers $n_1,n_2,n_3,\cdots and\ n_k$,
$(n_1+n_2+n_3+\cdots+n_k)!\ =\ (a_1\times a_2\times a_3\times\cdots\times a_{k-1})\times n_1!\times n_2!\times n_3!\times\cdots\times n_k!$,

$$\text{that is,}\left(\sum_{i=1}^{k}n_i\right)!=A\prod_{i=1}^{k}n_i\,!,$$

where $\mathrm{A}=a_1\times a_2\times a_3\times\cdots\times a_{k-1}$ and $A,a_1,a_2,a_3,\cdots,a_{k-1}$ are nonnegative integers.
Proof.
Let us begin the proof with example: (0+2+1+3)! =A× 0! ×2! ×1! ×3! ⟹720=120×0!×2!×1!×2!
and (0+0+0+1+0+0+0+0)! = A×0!×0!×0!×1!×0!×0!×0!×0! ⟹ 1 = A×1, where A = 1.

Let $x=\ n_2+n_3+n_4+\cdots+n_k\ .Then,(n_1+x)=a_1\times n_1!\times x!$ (refer to theorem 2.1),
that is, $(n_1+n_2+n_3+\cdots+n_k)!\ =\ a_1\times n_1!\times(n_2+n_3+\cdots+n_k)!$.

Similarly, if we apply the same way to prove each of the sums, we get as follows:
$(n_2+n_3+n_4+\cdots+n_k)!=a_2\times\ n_2!\times(n_3+n_4+\cdots+n_k)!;\ \ (n_3+n_4+n_5+\cdots+n_k)!=$
$a_3\times\ n_3!\times(n_4+n_5+\cdots+n_k)!;(n_4+n_5+n_6+\cdots+n_k)=a_4\times\ n_4!\times(n_5+n_6+\cdots+$
$n_k)!;\ ,\cdots,and\ (n_{k-1}+n_k)=a_{k-1}\times\ n_{k-1}!\times n_k.$

If we substitute these results step by step in $a_1\times n_1!\times(n_2+n_3+\cdots+n_k)!$, that is,
$a_1\times n_1!\times(n_2+n_3+n_4\cdots+n_k)!=\ a_1\times n_1!\times(a_2\times n_2!\times(n_3+n_4\cdots+n_k)!)$
$=a_1\times a_2\times n_1!\times n_2!\times(a_3\times n_3!\times(n_{4+}\cdots+n_k)!)$, etc. , we obtain the following result.

$(n_1+n_2+n_3+\cdots+n_k)!\ =\ (a_1\times a_2\times a_3\times\cdots\times a_{k-1})\times n_1!\times n_2!\times n_3!\times\cdots\times n_k!$,

$$\text{that is,}\left(\sum_{i=1}^{k}n_i\right)!=A\prod_{i=1}^{k}n_i\,!,$$

where $\mathrm{A}=a_1\times a_2\times a_3\times\cdots\times a_{k-1}$ and $A,a_1,a_2,a_3,\cdots,a_{k-1}$ are nonnegative integers.
Hence, theorem is proved.

For instance, if $n_1=n_2=n_3=\cdots=n_k=n$, then, $(n_1+n_2+n_3+\cdots+n_k)!=(k\times n)!$.,
where k, $n\geq 0$ are any integer, that is, k & n = 0, 1, 2, 3, 4, 5, ...,

If $n_1=n_2=n_3=\cdots=n_k=0$. Then, $(n_1+n_2+n_3+\cdots+n_k)!=(k\times 0)!=1$.
If $n_1=n_2=n_3=\cdots=n_k=1$. Then, $(n_1+n_2+n_3+\cdots+n_k)!=(k\times 1)!=k!$.
If $n_1=n_2=n_3=\cdots=n_k=k$. Then, $(n_1+n_2+n_3+\cdots+n_k)!=(k\times k)!=k^2!$.

Theorem 2.3: $\prod_{i=1}^{k}(n_i!)^r = \frac{1}{A^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r$, where $A, r \geq 1, a_i \geq 0$ are integers.

Proof. This theorem is proved by using the following theorem:

$\left(\sum_{i=1}^{k} n_i\right)! = A\prod_{i=1}^{k} n_i\,!$, where $A = \prod_{i=1}^{k-1} a_i$ and $A \geq 1$ & a_i are integers.

$$\left(\sum_{i=1}^{k} n_i\right)! = A\prod_{i=1}^{k} n_i! \Longrightarrow \left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r = \left(A\prod_{i=1}^{k} n_i\,!\right)^r = A^r\left(\prod_{i=1}^{k} n_i\,!\right)^r = A^r\prod_{i=1}^{k}(n_i!)^r.$$

From this expression, we get $\prod_{i=1}^{k}(n_r!)^r = \frac{1}{A^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r$.

Hence, theorem is proved.

Theorem 2.4: $\sum_{i=1}^{k}(n_i!)^r = \frac{1}{B^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r$, where $B, r \geq 1$ & $a_i \geq 0$ are integers.

Proof. This theorem is proved by using the theorem 2.1 as follows:

$\left(\sum_{i=1}^{k} n_i\right)! = A\prod_{i=1}^{k} n_i\,!$, where $A = \prod_{i=1}^{k-1} a_i$ and $A \geq 1$ & a_i are integers.

Since $\sum_{i=1}^{k} n_i\,! \leq \prod_{i=1}^{k} n_i\,!$, we can obtain $\left(\sum_{i=1}^{k} n_i\right)! = B\sum_{i=1}^{k} n_i\,!$, where $B \geq 1$ is an integer.

Thus, $\prod_{i=1}^{k}(n_i!)^r = \frac{1}{A^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r \Rightarrow \sum_{i=1}^{k}(n_i!)^r = \frac{1}{B^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r$.

Hence, theorem is proved.

This idea can help to the researchers working in computational science, management, science, and engineering.

3. Machine Learning and Cybersecurity

Artificial Intelligence built on machine learning algorithms that are handling data of various types is the simulation of human mind in machines. Data analysis in machine-learnings is the process of inspecting, cleansing, transforming, and modelling data with the goal of discovering useful information and decision making. The machine learning algorithms are built on mathematical and combinatorial techniques [10-12] such mean, median, mode, standard

deviation and variance, linear and polynomial regressions, binomial and probability distribution, decision tree, etc. The computational and combinatorial techniques with traditional coefficient and optimized coefficient [13] are given below:

Binomial expansion and sereis: $\sum_{i=0}^{r} V_i^n x^i = \sum_{i=0}^{r} \prod_{j=1}^{n} \frac{i+j}{r!} x^i$ & $(x+y)^n = \sum_{i=0}^{n} V_i^{n-i} x^{n-i} y^i$.

Binomial and Probability distribution: $\mathrm{P(x)} = V_x^{n-x} p^x q^{n-x}$ & $\sum P(x) = 1, 0 \le P(x) \le 1$.

Binomial Identities and expansions: $V_0^n + V_1^n + V_2^n + V_3^n \cdots + V_{r-1}^n + V_r^n = V_r^{n+1}$,

$$\sum_{i=1}^{r} V_i^{n+1} = \sum_{i=0}^{r} V_i^0 + \sum_{i=0}^{r} V_i^1 + \sum_{i=0}^{r} V_i^2 + \sum_{i=0}^{r} V_i^3 + \cdots + \sum_{i=0}^{r} V_i^{n-1} + \sum_{i=0}^{r} V_i^n, \quad \text{and}$$

$$\sum_{i=0}^{r} V_i^{n+1} x^i = \sum_{i=0}^{r} V_i^n x^i + \sum_{i=1}^{r} V_{i-1}^n x^i + \sum_{i=2}^{r} V_{i-2}^n x^i + \cdots + \sum_{i=r-1}^{r} V_{i-(r-1)}^n x^i + \sum_{i=r}^{r} V_{i-r}^n x^i.$$

Polynomial Regression is a regression algorithm that models the relationship between a dependent(y) and independent variable(x) as nth degree polynomial. Decision tree is a supervised learning method that is used for both classification and regression.

Computational science is a rapidly growing multi-and inter-disciplinary area where science, engineering, computation, mathematics, and collaboration uses advance computing capabilities to understand and solve the most complex real-life problems [13-23]. Cybersecurity is the practice of protecting the computing systems, devices, networks, programs and data from cyber-attacks. Its objective is to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems and networks. For this purpose, we need a strong security mathematical algorithm like RSA algorithm and Elliptic Curve Cryptography. The factorials and binomial coefficients [8-12] enable computing science to build a strong cryptographic algorithm for the effective information security. The following factorial result can be used as power tool in algorithm and software development.

For any k nonnegative integers $n_1, n_2, n_3, \cdots and\ n_k$,

$$(n_1 + n_2 + n_3 + \cdots + n_k)! = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}) \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!,$$

$$\text{that is,} \left(\sum_{i=1}^{k} n_i \right)! = A \prod_{i=1}^{k} n_i\,!,$$

where $\mathrm{A} = a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}$ and $A, a_1, a_2, a_3, \cdots, a_{k-1}$ are nonnegative integers.

For example, (0+0+0+1+1+1+0+0+1+1+0)! = A× 0! ×0! ×0! ×1! × 1! ×1! ×0! × 0! ×1! ×1! ×0!, that is, 120=120× 0! ×0! ×0! ×1! × 1! ×1! ×0! × 0! ×1! ×1! ×0! $\Longrightarrow 120 = 120$, where $\mathrm{A} = 120$ and 0! ×0! ×0! ×1! × 1! ×1! ×0! × 0! ×1! ×1! ×0! =1. This may be vulnerability for the construction of algorithms. For designing the strong algorithm for application in cybersecurity, the integers or prime numbers of $n_1, n_2, n_3, \cdots, n_k$ must be greater than the integer 1.

4. Conclusion

In this article, combinatorial techniques such as factorials, binomial coefficients, and multinomial computations have been introduced for the applications in computational science,

artificial intelligence, and cryptography. These methodological advances can enable the researchers working in computational science, management, science and engineering to solve the most real life problems and meet today's challenges [16-23].

References

[1] Annamalai, C. (2022) Factorials and Integers for Applications in Computing and Cryptography. *COE, Cambridge University Press.* https://doi.org/10.33774/coe-2022-b6mks.

[2] Annamalai, C. (2022) Factorials, Integers, and Multinomials for Algorithms. *Zenodo*. https://doi.org/10.5281/zenodo.6976253.

[3] Annamalai, C. (2022) Factorials, Integers and Mathematical and Binomial Techniques for Machine Learning and Cybersecurity. *COE, Cambridge University Press.* https://doi.org/10.33774/coe-2022-b6mks-v2.

[4] Annamalai, C. (2022) Factorials, Integers, and Factorial Theorems for Computing and Cryptography. *OSF Preprints*. https://doi.org/10.31219/osf.io/xetuz.

[5] Annamalai, C. (2022) My New Idea for Optimized Combinatorial Techniques. *Zenodo.* https://doi.org/10.5281/zenodo.6626293.

[6] Annamalai, C. (2022) Intuitionistic Fuzzy Sets and Combinatorial Techniques in Computation and Weather Analysis. *engrXiv*. https://doi.org/10.31224/2387.

.

[7] Annamalai, C. (2022) Factorial of Sum of Nonnegative Integers for Computing and Algorithms. *Zenodo*. https://doi.org/10.5281/zenodo.6612724.

[8] Annamalai, C. (2022) Ascending and Descending Orders of Annamalai's Binomial Coefficient. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.4109710.

[9] Annamalai, C. (2022) Combinatorial Relation of Optimized Combination with Permutation. *SSRN Electronic Journal*. https://dx.doi.org/10.2139/ssrn.4057425.

[10] Annamalai, C. (2022) Theorems based on Annamalai's Binomial Coefficient and Identity. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.4109904.

[11] Annamalai, C. (2022) Differentiation and Integration of Annamalai's Binomial Expansion. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.4110255.

[12] Annamalai, C. (2022) Analysis of the Relationship between Integers and Factorial Functions. *OSF Preprints*. https://doi.org/10.31219/osf.io/r27s6.

[13] Annamalai, C. (2022) Application of Factorial and Binomial Identities in Communications, Information and Cybersecurity. *Research Square.* https://doi.org/10.21203/rs.3.rs-1666072/v6.

[14] Annamalai, C. (2022) Factorials, Integers and Multinomial Coefficients and its Computing Techniques for Machine Learning and Cybersecurity. *COE, Cambridge University Press*. https://doi.org/10.33774/coe-2022-b6mks-v3.

[15] Annamalai C (2020) "Combinatorial Optimized technique for Computation of Traditional Combinatorics", Jñānābha, Vol. 50(2), pp 128-131.

[16] Annamalai, C. (2012) Modelling exponential decay to predict half-life of radioactive substance. *Journal of Scientific and Mathematical Research*, Vol. 6, pp 1-3. https://doi.org/10.5281/zenodo.6614430.

[17] Annamalai, C. (2014) Intuitionistic Fuzzy Sets: New Approach and Applications. *International Journal of Research in Computer and Communication Technology*, Vol. 3(3), pp 283-285. http://ssrn.com/abstract=4100670.

[18] Annamalai, C. (2019) Algorithmic Computation of Annamalai's Geometric Series and Summability. *Mathematics and Computer Science*, Vol. 3(5), pp 100-101. https://doi.org/10.11648/j.mcs.20180305.11.

[19] Annamalai, C. (2017) Computational modelling for the formation of geometric series using Annamalai computing method. zbMath (Zbl 1391.65005); Jñānābha, Vol.47 (2) pp 327-330.

[20] Annamalai, C. (2019) Computation of Series of Series Using Annamalai's Computing Model. https://www.scopus.com/authid/detail.uri?authorId=57226408094#tab=preprints *Elsevier BV; SSRN* 15565068.

[21] Annamalai, C. (2022) Computational and Numerical Methods for Combinatorial Geometric Series and its Applications. *COE, Cambridge University Press.* https://doi.org/10.33774/coe-2022-pnx53-v21.

[22] Annamalai, C. (2022) Computing Method for Combinatorial Geometric Series and Binomial Expansion. *SSRN* 4168016. http://dx.doi.org/10.2139/ssrn.4168016.

[23] Annamalai, C. (2010) Application of Exponential Decay and Geometric Series in Effective Medicine. *Advances in Bioscience and Biotechnology*, Vol. 1(1), pp 51-54. https://doi.org/10.4236/abb.2010.11008.