Computation of Combinatorial Geometric Series and its Combinatorial Identities 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: Combinatorial techniques with binomial coefficients, factorials and multinomial computation are used as computing algorithm or cryptographic algorithm 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 this article, combinatorial geometric series is discussed more for the application of machine learning and cybersecurity.

MSC Classifications Codes: 05A10, 40A05 (65B10)

Keywords: algorithm, combinatorics, computation, multinomial

1. Introduction

Binomial and probability distribution and combinatorial techniques [1-18] 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 [6-18] 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.

2. Combinatorial Geometric Series

The combinatorial geometric series [1-5] is derived from the multiple summations of geometric series. The coefficient of each term in the combinatorial denotes the binomial coefficient V_n^r.

$$\sum_{i_1=0}^{n}\sum_{i_2=i_1}^{n}\sum_{i_3=i_2}^{n}\cdots\sum_{i_r=i_{r-1}}^{n} x^{i_r} = \sum_{i=0}^{n} V_i^r x^i \ \ \& \ \ V_n^r = \frac{(n+1)(n+2)(n+3)\cdots(n+r-1)(n+r)}{r!},$$

where $n \geq 0, r \geq 1 \ and \ n, r \in N = \{0, 1, 2, 3, \cdots\}$.

Here, $\sum_{i=0}^{n} V_i^r x^i$ denotes the combinatorial geometric series and V_n^r the binomial coefficient.

The traditional binomial coefficient denotes $\binom{n}{r} = nCr = \frac{n!}{r!\,(n-r)!}$, where $n, r \ \in N$.

The factorial function or factorial of a nonnegative integer n, denoted by $n!$, is the product of all positive integers less than or equal to n. For examples, $5! = 1\times2\times 3\times4\times5 = 120$ and $0! = 1$.

Theorem 2.1: $\frac{(n+r)!}{n!\,r!} = \prod_{i=1}^{r} \frac{n+i}{r!} = V_n^r$, where $n, r \geq 0$ & $n, r \in N$.

$Proof.\binom{n+r}{n} = \frac{(n+r)!}{n!\,(n+r-n)!} = \frac{(n+r)!}{n!\,r!} = \frac{(n+1)(n+2)(n+3)\cdots(n+r)}{r!} = V_n^r.$

That is, $V_n^r = \frac{(n+1)(n+2)(n+3)\cdots(n+r)}{r!} = \prod_{i=1}^{r} \frac{n+i}{r!}.$

From the above expressions, we conclude that

$$\frac{(n+r)!}{n!\,r!} = \prod_{i=1}^{r} \frac{n+i}{r!} = V_n^r, \text{where } n, r \geq 0 \ \ \& \ \ n, r \in N.$$

Note that $(n+r)! = V_n^r n!\,r! \Longrightarrow (2n)! = 2V_{n-1}^n (n!)^2$.

The combinatorial or binomial identities of V_r^n are derived from Theorem 2.1 as follows:
(i) $V_n^0 = V_0^n = 1$ for $n = 0, 1, 2, 3, \cdots$
(ii) $V_r^m = V_m^r$, $(m, r \geq 1$ & $m, r \in N)$.

$Proof$ for identity (i): $V_n^0 = V_0^n = \frac{(0+n)!}{0!\,n!} = 1 \Longrightarrow \quad V_0^0 == \frac{(0+0)!}{0!\,0!} = 1.$

$Proof$ for identity (ii): $V_n^m = V_m^n = \frac{(m+n)!}{m!\,n!}.$

Theorem 2.2: $\frac{(n+p+r)!}{n!\,p!\,r!} = V_n^{p+r} \times V_p^r$, where $n, p, r \in N$.

$Proof: V_n^{p+r} \times V_p^r = \times \frac{(n+p+r)!}{n!\,(p+r)!} \times \frac{(p+r)!}{p!\,r!} = \frac{(n+p+r)!}{n!\,p!\,r!}.$

Theorem 2.3 : For any k nonnegative integers $n_1, n_2, n_3, \cdots$ and n_k,
$(n_1 + n_2 + n_3 + \cdots + n_k)! = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1})(n_1!\,n_2!\,n_3! \cdots n_k!)$,
where $a_1 = V_{n_1}^{n_2+n_3+n_4+\cdots+n_k}, a_2 = V_{n_2}^{n_3+n_4+\cdots+n_k}, a_3 = V_{n_3}^{n_4+n_5+\cdots+n_k}, \cdots, a_{k-1} = V_{n_{k-1}}^{n_k}$ and
$n_i \geq 0; a_i \geq 1$ for $i = 1, 2, 3, \cdots, k$ and $n_i, a_i \in N = \{0, 1, 2, 3, \cdots, \}$.

$$Proof.\, a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1} = V_{n_1}^{n_2+n_3+n_4+\cdots+n_k} \times V_{n_2}^{n_3+n_4+\cdots+n_k} \times V_{n_3}^{n_4+n_5+\cdots+n_k} \times \cdots \times V_{n_{k-1}}^{n_k}$$

$$= \frac{(n_1+n_2+n_3+\cdots+n_k)!}{n_1!\,(n_2+n_3+\cdots+n_k)!} \times \frac{(n_2+n_3+\cdots+n_k)!}{n_2!\,(n_3+n_4+\cdots+n_k)!} \times \frac{(n_3+n_4+\cdots+n_k)!}{n_3!\,(n_4+n_5+\cdots+n_k)!} \times \cdots \times \frac{(n_{k-1}+n_k)!}{n_{k-1}!\,n_k!} = \frac{(n_1+n_2+n_3+\cdots+n_k)!}{n_1!\,n_2!\,n_3! \cdots n_k!}.$$

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

From this expression, we conclude that
$(n_1 + n_2 + n_3 + \cdots + n_k)! = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1})(n_1!\, n_2!\, n_3! \cdots n_k!)$.

In the short form, we can write this theorem as follows:
$(n_1 + n_2 + n_3 + \cdots + n_k)! \;=\; (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}) \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!$,

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

where $\mathrm{A} = a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}$ & $n_i \geq 0; a_i \geq 1$ for $i = 1, 2, 3, \cdots, k$ *and* $n_i, a_i \in N$.

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 2.4: $2\dfrac{(2n-1)!}{n!\,(n-1)!} = \dfrac{(2n)!}{(n!)^2}$, where $n, \geq 1$ & $n \in N$.

$$Proof.\; V_n^n = \frac{(n+1)(n+2)(n+3)\cdots(n+n-1)(n+n)}{n!}$$
$$= 2\frac{(n)(n+1)(n+2)(n+3)\cdots(n+n-1)}{n!} = 2V_{n-1}^n, \qquad i.e., 2V_{n-1}^n = V_n^n.$$

By applying Theorem 2.1 to $2V_{n-1}^n = V_n^n$, we get $2\dfrac{(2n-1)!}{n!\,(n-1)!} = \dfrac{(2n)!}{(n!)^2}$ $\left(\because V_n^r = \dfrac{(n+r)!}{n!\,r!}\right)$.
Hence, theorem is proved.

Theorem 2.5: $\displaystyle\prod_{i=1}^{k}(n_i!)^r = \frac{1}{A^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r$, where $A, r \geq 1, a_i \geq 0$ are integers.

Proof. This theorem is proved by using the following theorem:
$\displaystyle\left(\sum_{i=1}^{k} n_i\right)! = A\prod_{i=1}^{k} n_i\,!$, where $\displaystyle A = \prod_{i=1}^{k-1} a_i$ and $A \geq 1$ & a_i are integers.

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

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

Theorem 2.6: $\sum_{i=1}^{k}(n_i!)^r = \frac{1}{B^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r$, 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, $\prod_{i=1}^{k}(n_i!)^r = \frac{1}{A^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r \Longrightarrow \sum_{i=1}^{k}(n_i!)^r = \frac{1}{B^r}\left\{\left(\sum_{i=1}^{k} n_i\right)!\right\}^r$.

Hence, theorem is proved.

Theorem 2.7: $(p^n)! = I_n \times (p!)^n$, where $n, I_n \geq 1; p \geq 0$ & n, p, I_n are integers.

$Proof.\binom{p+q}{p} = \frac{(p+q)!}{p!\,q!} = I$, where $I \geq 1$ & I is an integer.

$(p+q)! = I \times p!\,q! \Longrightarrow (p \times q)! = I_1 \times p!\,q!$ since $(p \times q)! \geq (p+q)!$.

Let $q = p$. Then $(p \times p)! = I_2 \times p!\,p! \Longrightarrow (p^2)! = I_2 \times (p!)^2$.

$(p^3)! = I_3 \times (p!)^3$. Here, $(p^2)! \geq (p!)^2 \Longrightarrow (p^3)! \geq (p!)^3$, where $p \geq 0$ & p is an integer.

$(p^{n-1})! = I_{n-1} \times (p!)^{n-1} \Longrightarrow (p^n)! = I_n \times (p!)^n$, where $\mathrm{n} \geq 1$; $p \geq 0$ & n, p are integers.

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 [1-18] 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 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: $\mathrm{P(x)} = V_x^{n-x} p^x q^{n-x}$ & $\sum P(x) = 1, 0 \leq P(x) \leq 1$.

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

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

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

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. 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 [6-18] 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.

References

[1] Annamalai, C. (2022) Binomial Coefficients in Combinatorial Geometric Series and its Combinatorial Identities. *OSF Preprints*. https://doi.org/10.31219/osf.io/sv26w.

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

[3] 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.

[4] 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.

[5] Annamalai, C. (2022) Computation Method for Combinatorial Geometric Series and its Applications. *COE*, *Cambridge University Press.* https://doi.org/10.33774/coe-2022-pnx53-v22.

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

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

[8] 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.

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

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

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

.

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

[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. (2022) Multinomial Computation and Factorial Theorems for Cryptographic Algorithm and Machine Learning. *COE, Cambridge University Press*. https://doi.org/10.33774/coe-2022-b6mks-v4.

[16] Annamalai, C. (2022) Multinomial Computation and Factorial Theorems for Artificial Intelligence and Cybersecurity. *COE, Cambridge University Press*. https://doi.org/10.33774/coe-2022-b6mks-v5.

[17] Annamalai, C. (2022) Combinatorial Techniques and Multinomial Theorems with Factorials for Machine Learning and Cybersecurity. *COE, Cambridge University Press*. https://doi.org/10.33774/coe-2022-b6mks-v6.

[18] Annamalai, C. (2022) Computation of Combinatorial Geometric Series and its Combinatorial Identities for Machine Learning and Cybersecurity. *COE, Cambridge University Press*. https://doi.org/10.33774/coe-2022-b6mks-v7.