Volume: 14 Issue: 01 Pages: 5258-5260(2022) ISSN: 0975-0290

Application of Factorial and Binomial Identities in Information, Cybersecurity and Machine Learning

ChinnarajiAnnamalai
Department of Management, Indian Institute of Technology, Kharagpur-2
Email: anna@iitkgp.ac.in

ABSTRACT

This paper presents application of the binomial and factorial identities and expansions that are used in artificial intelligence, machine learning, and cybersecurity. The factorial and binomial identities can be used as methodological advances for various algorithms and applications in information and computational science. Cybersecurity is the practice of protecting the computing systems, communication networks, data and programs 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 purposes, we need a strong cryptographic algorithms like RSA algorithm and Elliptic Curve Cryptography. In this connection, computing and combinatorial techniques based on factorials and binomial distributions are developed for the researchers who are working in artificial intelligence and cybersecurity.

Keywords - **Cybersecurity, combinatorics, computation, factorial, information.**

Date of Submission: Jun 17, 2022 Date of Acceptance: Jul 16, 2022

I. INTRODUCTION

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. Wireless communication is not fully secure for transmission of information in a peer-to-peer network, that is, some information leakage through the transmission of wireless signal is unavoidable. In this case, cybersecurity is the practice of protecting the computing systems, devices, communication networks, programs and data from cyber-attacks. The aim of this article is to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems and networks. For this purposes, we need a strong security mathematical algorithm like RSA algorithm and Elliptic Curve Cryptography. The factorial [1, 2] and binomial theorem [3-7] will help to build a strong artificial intelligence-based cryptographic algorithm.

II. THEOREM IN FACTORIALS

The factorial of a non-negative integer *n*, denoted by *n*!, is the product of all positive integers less than or equal to *n*. For example, $4! = 1 \times 2 \times 3 \times 4 = 24$ and $0! = 1$.

Theorem in Factorials [11] : $(n_1 + n_2 + n_3 + \cdots + n_k)! = T \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!$, where $T, n_i \in N = \{1, 2, 3, \cdots\}$ & $i = 1, 2, 3, \cdots, k$.

Proof: Let $x = n_2 + n_3 + \cdots + n_k$.
$(n_1 + x)! = n_1! \times (n_1 + 1)(n_1 + 2)(n_1 + 3) \cdots (n_1 + x)$.
We know that $(r + 1)(r + 2)(r + 3) \cdots (r + n)$
$= a \times n!$, where a is a positive integer.
For example,
Let $n = 5$ and $r = 3$.
Then, $(3 + 1)(3 + 2)(3 + 3)(3 + 4)(3 + 5)$
$= 6720 = 56 \times 120 = 56 \times 5!$ and

$$(5 + 1)(5 + 2)(5 + 3) = 336 = 56 \times 6.$$

From the above result, we get $n_1! \times (n_1 + 1)(n_1 + 2)(n_1 + 3) \cdots (n_1 + x) = a_1 \times n_1! \times x!$,
$i.e., (n_1 + x)! = a_1 \times n_1! \times x! = a_1 \times n_1! \times (n_2 + n_3 + \cdots + n_k)!$ $(\because x = n_2 + n_3 + \cdots + n_k)$.

Similarly, if we continue the same process up to k-1 times, then we obtain the result: $(n_1 + n_2 + n_3 + \cdots + n_k)! = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}) \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!$.

Let $T = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1})$,
where $T, a_i \in N = \{1, 2, 3, \cdots\}$ & $i = 1, 2, 3, \cdots, k - 1$.

Then, $(n_1 + n_2 + n_3 + \cdots + n_k)! = T \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!$.

Hence, theorem is proved.

III. ARTIFICIAL INTELLIGENCE-BASED CYBERSECURITY

The mathematical results mentioned-below can be used as an application in the artificial intelligence-based cybersecurity and these results also help to create a strong security algorithm like RSA algorithm and Elliptic Curve Cryptography in the field of cybersecurity in order toreduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems and networks.

We have already understood the below factorial identity and detailed proof in the previous section of this paper. Now, we find how to use this result in another way.

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

that is, $(n_1+n_2+n_3+\cdots+n_k)!$
$= T\times n_1!\times n_2!\times n_3!\times\cdots\times n_k!$.
Here, $n_1, n_2, n_3, \cdots, n_k$ are possitive integers.

An alternative way for finding the positive integer T is given below:

$$T=\frac{(n_1+n_2+n_3+\cdots+n_k)!}{n_1!\times n_2!\times n_3!\times\cdots\times n_k!},$$

where $T, n_i \in N=\{1,2,3,\cdots\}\ \&\ i=1,2,3,\cdots$

For our convenience, we can rearrange the positive integers that are equal to the product T.
Let $T=64$. $T=1\times 64$; $T=2\times 32$;
$T=2\times 2\times 16$; $T=2\times 4\times 8$; $T=4\times 4\times 4$; etc.
Similarly, if $T=21$, Then,
$T=1\times 21$ *or* $T=3\times 7$.

3.1 Binomial Identities

Binomial identities [3-13] mentioned below can be used in cybersecurity:

(1) $V_r^n=V_n^r (n,r\geq 1)$. (2) $V_r^{n+1}-V_r^n=V_{r-1}^n$.
(3) $1+V_1^1+V_1^2+V_1^3\cdots\cdots V_1^n=V_2^n$. (4) $V_n^n=2V_{n-1}^n$.
(5) $V_0^n+V_1^n+V_2^n+V_3^n\cdots+V_{r-1}^n+V_r^n=V_r^{n+1}$.

(6) $\sum_{i=0}^{n}(i+1)V_i^{n-i}=(n+2)2^{n-1}$.

(7) $\sum_{i=0}^{n} i\times V_i^{n-i}=n2^{n-1}$. (8) $\sum_{i=0}^{n}V_i^{n-i}=2^n$.

(9) $\sum_{i=0}^{n}(i-1)V_i^{n-i}=(n-2)2^{n-1}$.

(10) $V_1^1+V_2^2+V_3^3+\cdots+V_n^n$
$=2(V_0^1+V_1^2+V_2^3+\cdots+V_{n-1}^n)$.

(11) $$\sum_{i=1}^{r}V_i^{n+1}=\sum_{i=0}^{r}V_i^0+\sum_{i=0}^{r}V_i^1+\sum_{i=0}^{r}V_i^2+\sum_{i=0}^{r}V_i^3+\cdots+\sum_{i=0}^{r}V_i^n$$

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

The numerical expression of binomial coefficient used in binomial identities is given below:

$$V_r^n=\frac{(r+1)(r+2)(r+3)\cdots\cdots(r+n-1)(r+n)}{n!},$$

$(n,r\in N, n\geq 1, \&\ r\geq 0)$.

3.2 Computation of Sum of Binomial Coefficients

The computation of sum of binomial coefficients is developed by sing the binomial identity (10).

$$\prod_{i=1}^{1}\frac{(1+i)}{1!}+\prod_{i=1}^{2}\frac{(2+i)}{2!}+\prod_{i=1}^{3}\frac{(3+i)}{3!}+\cdots+\prod_{i=1}^{n-1}\frac{(n-1+i)}{(n-1)!}+\prod_{i=1}^{n}\frac{(n+i)}{n!}=$$

$$2\left(\prod_{i=1}^{1}\frac{(0+i)}{1!}+\prod_{i=1}^{2}\frac{(1+i)}{2!}+\prod_{i=1}^{3}\frac{(2+i)}{3!}+\cdots+\cdots+\prod_{i=1}^{n-1}\frac{(n-2+i)}{(n-1)!}+\prod_{i=1}^{n}\frac{(n-1+i)}{n!}\right)$$

$$\Rightarrow\sum_{j=1}^{n}\prod_{i=1}^{j}\frac{(j+i)}{j!}=2\sum_{j=1}^{n}\prod_{i=1}^{j}\frac{(j-i+i)}{j!}.$$

3.3 Relation between the Binomial Expansions with multiple of 2

Relation 1: $$\sum_{i=0}^{n}(i+1)V_i^{n-i}+\sum_{i=0}^{n}(i-1)V_i^{n-i}=\sum_{i=0}^{n}i\times V_i^{n-i}=n2^{n-1}.$$

Proof: Let us simply the general terms in the two parts of binomial expansions (Relation 1) as follows:
$(i+1)V_i^{n-i}+(i-1)V_i^{n-i}$
$=2iV_i^{n-i}$. This idea can be applied for Relation 1.

$$\sum_{i=0}^{n}(i+1)V_i^{n-i}+\sum_{i=0}^{n}(i-1)V_i^{n-i}=2\sum_{i=0}^{n}iV_i^{n-i}$$
$$=(n+2)2^{n-1}+(n-2)2^{n-1}$$
$$=2n2^{n-1}.$$

Then, $2\sum_{i=0}^{n}iV_i^{n-i}=2n2^{n-1}\Rightarrow\sum_{i=0}^{n}iV_i^{n-i}=n2^{n-1}$.

Relation 2: $$\sum_{i=0}^{n}(i+1)V_i^{n-i}-\sum_{i=0}^{n}(i-1)V_i^{n-i}=\sum_{i=0}^{n}V_i^{n-i}=2^n.$$

Proof: Let us simply the general terms in the two parts of binomial expansions (Relation 2) as follows:
$(i+1)V_i^{n-i}-(i-1)V_i^{n-i}$
$=2V_i^{n-i}$. This idea can be applied for Relation 2.

$$\sum_{i=0}^{n}(i+1)V_i^{n-i}-\sum_{i=0}^{n}(i-1)V_i^{n-i}=2\sum_{i=0}^{n}V_i^{n-i}$$
$$=(n+2)2^{n-1}-(n-2)2^{n-1}$$
$$=4\times 2^{n-1}.$$

Then, $2\sum_{i=0}^{n}V_i^{n-i}=22^n\Rightarrow\sum_{i=0}^{n}V_i^{n-i}=2^n$.

Hence, two relations are proved.

3.4 Computation of Binomial Expansions

Computation of binomial expansions [6 – 8] is constituted by using the binomial identity (12),

Volume: 14 Issue: 01 Pages: 5258-5260(2022) ISSN: 0975-0290

$$\sum_{i=1}^{r} V_i^{n+1} = \sum_{i=0}^{r} V_i^0 + \sum_{i=0}^{r} V_i^1 + \sum_{i=0}^{r} V_i^2 + \sum_{i=0}^{r} V_i^3 + \cdots + \sum_{i=0}^{r} V_i^{n-1} + \sum_{i=0}^{r} V_i^n \Rightarrow$$

$$\sum_{i=1}^{r} \frac{(i+1)(i+2)(i+3)\cdots(i+n)}{n!} = \sum_{i=0}^{r} \frac{1}{0!} + \sum_{i=0}^{r} \frac{(i+1)}{1!} + \sum_{i=0}^{r} \frac{(i+1)(1+2)}{2!} + \cdots + \sum_{i=0}^{r} \frac{(i+1)(i+2)(i+3)}{3!} + \cdots + \sum_{i=0}^{r} \frac{(i+1)(i+2)(i+3)\cdots(i+n-1)}{(n-1)!}.$$

3.5 Summation of Binomial Series

The following binomial series [7] is constituted based on the binomial identity (13).

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

Proof: Let's show that the computation of addition of binomial series (right-hand side) is equal to the sum of binomial series for upper limit r+1(left-hand side).

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

$$= (V_0^n + V_1^n x + V_2^n x^2 + V_3^n x^3 + \cdots + V_r^n x^r) + (V_0^n x + V_1^n x^2 + V_2^n x^3 + V_3^n x^4 + \cdots + V_{r-1}^n x^r) + (V_0^n x^2 + V_1^n x^3 + V_2^n x^4 + V_3^n x^5 + \cdots + V_{r-2}^n x^r) + \cdots + (V_0^n x^{r-1} + V_1^n x^r) + V_0^n x^r$$

$$= V_0^n + (V_0^n + V_1^n)x + (V_0^n + V_1^n + V_2^n)x^2 + \cdots + (V_0^r + V_1^r + V_2^r + V_3^r + \cdots + V_n^r)x^r$$

(Note that $V_0^p + V_1^p + V_2^p + \cdots + V_r^p = V_r^{p+1}$ and $V_0^p = V_0^{p+1} = 1$)

$$= V_0^{n+1} + V_1^{n+1} x + V_2^{n+1} x^2 + V_3^{n+1} x^3 + V_4^{n+1} x^4 + \cdots + V_{r-1}^{n+1} x^{r-1} + V_r^{n+1} x^r = \sum_{i=0}^{r} V_i^{n+1} x^i.$$

Hence, it is proved.

IV. CONCLUSION

In this article, a mathematical techniques and applications [15] for an artificial intelligence-based cybersecurity have been introduced in order to protect the computing systems, devices, networks, programs and data from cyber-attacks, that is, to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, programs, and networks. The factorial and binomial identities and expansions can be used as artificial intelligence-based methodological advance in cybersecurity.

REFERENCES

[1]McCulloch J F (1888) "A Theorem in Factorials", Annals of Mathematics, 4(5), 161-163. https://doi.org /10.2307/1967449.

[2]Bhargava M (2008) "The Factorial Function and Generalizations", the American Mathematical Montly, 107(9),783 – 199.https://doi.org/10.2307/2695734

[3]Annamalai C (2020) "Optimized Computing Technique for Combination in Combinatorics", hal-0286583. https://doi.org/10.31219/osf.io/9p4ek.

[4]Annamalai C (2020) "Novel Computing Technique in Combinatorics", hal-02862222.https://doi.org/10.31219/ osf.io/m9re5.

[5]Annamalai C (2022) "Comparison between Optimized and Traditional Combinations of Combinatorics", OSF Preprints.https://doi.org/10.31219/osf.io/2qdyz.

[6]Annamalai C (2022) "Novel Binomial Series and its Summations", Authorea Preprints.https://doi.org/ /au.164933885.53684288/v2.

[7]Annamalai C (2022) "Annamalai's Binomial Identity and Theorem", SSRN Electronic Journal. http://dx.doi.org /10.2139/ssrn.4097907.

[8]Annamalai C (2022) "Sum of Summations of Annamalai's Binomial Expansions", ZenodoPrepints. https://doi.org/10.5281/zenodo.6582700.

[9]Annamalai C (2022) "Combinatorial Theorem for Multiple of Two with Exponents", OSF Preprints. https://doi.org/10.31219/osf.io/awu6b.

[10]Annamalai C (2022) "Combinatorial Relation of Optimized Combination with Permutation", Zenodo. https://doi.org/10.5281/zenodo.6341590.

[11]Annamalai C (2022) "Application of Factorial and Binomial identities in Cybersecurity", engrXiv. https://doi.org/10.31224/2355.

[12]Annamalai C (2022) "A Binomial Expansion equal to Multiple of 2 with Non-Negative Exponents", OSF Preprints.https://doi.org/10.31219/osf.io/73quz.

[13]Annamalai C (2022) "Computation of Binomial Expansions and Application in Science and Engineering", engrXiv. https://doi.org/10.31224/2373.

[14]Annamalai C (2022) "Computation of Sum of Optimized Binomial Coefficients and Application in Computational Science and Engineering, ZenodoPrepints, https://doi.org/10.5281/zenodo.6589551.

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