International Journal of Advances in Mathematics
Volume 2018, Number 2, Pages 83-89, 2018
eISSN 2456-6098

Recursive generation of prime numbers in the space of discrete geometries

Yury Grigoryan[1], Yeghisabet Alaverdyan*
[1,*]State Engineering University of Armenia, 105 Teryan Str., Yerevan 0009, Armenia.
* E-mail: yurgrig@yahoo.com; ealaverdjan@gmail.com

ABSTRACT. New method of generating prime numbers through quantization of discrete geometrical space is proposed. It is shown that quantization of the geometrical space results in stratification of the space into subspaces in such a way that to each subspace a distinct indivisible line is associated. The peculiarity of the method is that the indivisible lines, newly defined, are derived based on prime numbers. The paper introduces also a recurrence relation providing the combinatorial mechanism of generating primes in the discrete geometrical space, which makes it possible to estimate the efficiency of the proposed method versus the existing probabilistic algorithms.

1. Introduction

The axiomatic of inhomogeneous geometry considered in Ref. [1] showed that there exists a general number-theoretical method of representing three different geometries, such as Euclidean, non Euclidean and Projective, in a unified metric space. The works [2, 3] introduce the concepts of arithmetical coding of discrete objects in terms of arithmetic graphs. Based on the concepts, a definite arithmetical set of integers is constructed, a metric is introduced, and the statement, that the set is a metric space, has been proven. The discrete geometrical space answers to one of the open problems in discrete mathematics, concerned with the existence of indivisible lines, where the ends, x, y, are the only points [4] located on due to the presence of the kernel in the space [2]. Besides, an association between indivisible lines and generation of infinite number of primes has been introduced [5, 6]. Generation of primes is an open problem in Number theory with regard of discovering some order in their sequence and distribution. Despite their simple definition, prime numbers seem to obey no other law than that of chance.

* Corresponding Author.
Received September 24, 2017; accepted February 17, 2018.
2010 Mathematics Subject Classification: 10A25,10H15
Key words and phrases: Arithmetic graph, discrete geometry, indivisible lines, prime numbers

2. Mathematical preliminaries

The geometric space $\mathfrak{R}(D)$, introduced in Ref. [2, 3], possesses an important property of a numerical axis for which the concepts of a point and its coordinate coincide. This circumstance makes it possible to considerably compress the amount of information on underlying geometrical and topological objects. Formulation of the concepts of points, discrete straight lines, discrete pseudo-straight lines, discrete planes and discrete extended planes, also of discrete limiting planes, have been formulated in Ref. [2, 3]. The planes obtained possess the property of inclusion of one plane into another, and this property combines them into a system, which, on the whole, testifies to the presence of a unified number-theoretic basis of the geometries considered.

Notion of arithmetic graphs arose when solving problems in theory of Boolean functions' disjunctive normal forms, concerned with arithmetical procedures of their minimization leading to specific encoding of graphs [7, 8]. On the other hand, construction of a complete set of symmetries, also the realizability of discrete objects, such as: graphs, Boolean functions, polyhedra, logic circuits, matrices, etc, in natural spaces stand for actual problems in the fields of mathematical modelling. Development of the theory of arithmetic graphs led also to the need for a more detailed study of arithmetical representation of simple cycles' of length $2p$ (p being a prime number), with the focus on the structure of their group of automorphisms [9].

Definition 1.[10]. A pair $G(N, M)$, where N stands for the set of vertices, and the pair (n_i, n_j), $n_i, n_j \in N$ if and only if $n_i + n_j \in M$, M being a generating set, is called an arithmetical graph, and any number of type $n_i + n_j = m$ is the label of the respective edge (n_i, n_j).

It was shown in Ref. [11] that the notions of arithmetical and simple graphs are equivalent in their classical essence. Anyway, $G(N|M)$ is used to denote arithmetical graphs, in order to explicitly distinguish these two notions.

Definition 2.[2]. A graph G is called a natural arithmetic graph, if it can be presented through an arithmetic graph as follows:

$$G(N_p|M), N_p = \{1, 2, \cdots, p\}, \quad M \subset \mathfrak{W}\{3, 4, \cdots, 2p-1\}. \tag{2.1}$$

Otherwise, the arithmetical graph is not natural.

Definition 3 [3]. The set of real numbers $\{\mathfrak{R} \setminus \{0\}\}$ is called an asymmetric set, if there exists at least one element $A \in \mathfrak{R} : -A \notin \mathfrak{R}$. Zero is excluded from consideration, as, by definition, it has no inverse in the set of real numbers.

Definition 4 [3]. A parametric set of real numbers

$$\Re(D) = \{D\} \cup (|D|, \infty) \tag{2.2}$$

with a fixed $D < 0$, is called a D-asymmetric set.

Notice that any set $\Re(D)$ is asymmetric with respect to its particular element D, and this very circumstance creates a premise for stratification of the geometrical space. For the purpose, let we fix an integer number $D \leqslant -2$,

and then consider the infinite parametric set

$$\aleph(D) = \{D, -D+1\} \cup \{D^2 - D + i\}, \quad i = 0, 1, 2, \cdots \ , \tag{2.3}$$

where the set $\aleph(D)$ stands for a discrete sample of the D-asymmetric set $\Re(D)$ from (2).

It is worthy to notice that the area of the triangle given by the three points, $D, -D+1, D^2 - D + i, i = 0, 1, 2,$, is as follows: $S = 1/2\sqrt{i}$, and is independent of the parameter D[3].

Theorem 1. *The parametric set of integers $\aleph(D)$ from (3) for any $D \leqslant -2$ is a D-asymmetric set.*

In Ref. [2] is shown that the set $\Re(D)$ with a fixed $D \leqslant -2$ forms an asymmetric metric space with a metric

$$r(A, B) = \begin{cases} \sqrt{A + B}\ , & A \neq B \\ 0\ , & A = B \end{cases}\ , \tag{2.4}$$

which points out to the existence of a zero-dimensional infinite metric space, i.e. the notion of the point coincides with the notion of its coordinate. This abstraction allows to eliminate the necessity to store coordinates in order to allocate the point in the space, and this is independent of the coordinating system under consideration.

Definition 5 [2]. Any integer $X \in \aleph(D_0)$ with a fixed $D \leqslant -2$ from (3) is called a point of the discrete geometric space $\aleph(D_0)$.

Definition 6 [2]. With a fixed integer $D \leqslant -2$, a pair of integers $(X, Y), X, Y \in \aleph(D_0)$ is called a discrete straight line, if the following holds:

1) $\sqrt{X + Y}$ is an integer.

2) There exists such an integer $Z \in \aleph(D_0)$ to satisfy the following:

$$XZ + YZ + XY = 0 \tag{2.5}$$

Definition 7[5]. With a fixed integer $D \leqslant -2$, the discrete straight line $(K, D_0), K, D_0 \in \aleph(D_0)$, is called the basic discrete straight line, if the following holds:

1) $K + D_0 = 1$,

2) There exists such a positive integer $C \in \aleph(D_0)$ to satisfy the following:

$$KD_0 + CD_0 + CK = 0. \tag{2.6}$$

For any fixed $D_0 \in \aleph(D_0)$ in Ref. [2], the notion of the three different planes, $\varepsilon, \bar{\varepsilon}, P$ with own specific definition points are introduced:

$$\varepsilon\{A, B, K, D_0, \}, \bar{\varepsilon}\{A, B, K, D_0, C\}, P\{A, B, K, D_0, C, E, F\}, \tag{2.7}$$

which are called discrete, discrete extended and boundary discrete planes, respectively. The planes so derived can be represented through the system of six equations with seven unknowns, as follows:

$$\left.\begin{array}{r} \left.\begin{array}{r} A+D_0=B+K \\ AD_0+BK=0 \\ K+D_0=1 \end{array}\right\}\varepsilon \\ KC+D_0C+KD_0=0 \end{array}\right\}\bar{\varepsilon} \quad \left.\begin{array}{r} \\ \\ \\ \\ K^2+{D_0}^2+C^2=E^2 \\ A^2+B^2+C^2=F^2 \end{array}\right\}P \tag{2.8}$$

Notice that the space itself is being compressed with each upcoming restriction introduced in (8).

With a fixed value of the parameter $D \leqslant -2$, each of the subsystem $\varepsilon,\ \bar{\varepsilon},\ P$ from (8) has a unique integral solution (9), expressed through an odd parameter $n = 1 - 2D_0$ $(n \geqslant 5)$:

$$\begin{gathered} D_0 = -\frac{n-1}{2},\ K = \frac{n+1}{2},\ C = \frac{n^2-1}{4}, \\ E = \frac{n^2+3}{4}, B = \frac{n(n-1)}{2},\ A = \frac{n(n+1)}{2},\ F = \frac{3n^2+1}{4}, \end{gathered} \tag{2.9}$$

satisfying the following condition:

$$\varepsilon \subset \bar{\varepsilon} \subset P. \tag{2.10}$$

Integral type of the above solutions is mostly important especially with regard to their use in coding theory.

Definition 8 [6]. The set $P\{D_0, K, A, B, C, E, F\}$ with a fixed point $D \leqslant -2$ is called the kernel of the space (3), if there exists such a perfect number $H \in \aleph(D_0)$ to satisfy the following:

$${D_0}^2 + K^2 + A^2 + B^2 + C^2 + E^2 + F^2 = H^2. \tag{2.11}$$

There were shown in Ref. [6] that the diofant equation (11) has an integer solution, which testifies to the existance of the kernel in the space (3). Note that (11) stands for the generalized case of the Pythagorean theorem. By using (8), the equation (11) is solved for $D_0 = -2, K = 3$, and $H = 2^{|D_0|}(2^K - 1) = 28$.

In the above considerations, the odd parameter $n = 1 - 2D_0 \geqslant 5$, in essence stratifies (quantize) the whole space $\aleph(D)$ (3) into an infinite number of subspaces $\aleph(D_0)$, all of them satisfying (8). The solution of (8) provides the existence of three distinct geometries, $\varepsilon \subset \bar{\varepsilon} \subset P$. For any fixed integer $D \in (-\infty, -2]$, an infinite and asymmetric set of integers is given in (3).

Definition 9 [2]. For any fixed $D = D_0 \in (-\infty, -2]$ the infinite set $\aleph(D_0)$ (3) is called D_0 - cut of the sub-space $\aleph(D)$.

Now it is time to introduce the definition of indivisible lines in the space of discrete geometries.

Definition 10 [5]. The pair of points $(D_0, |D_0| + 1) = (D_0, K_0) \in \aleph(D_0)$ satisfying the following two conditions,

$$D_0 + K_0 = 1 \tag{2.12}$$

$${D_0}^2 + {K_0}^2 = p_0 \tag{2.13}$$

is called an indivisible line of the D_0 - cut corresponding to $\aleph(D_0)$, where $p_0 = 60m + 1$ is a prime number.

It follows from (12) that for any positive odd number $p_0 = 1 - 2D_0 \geqslant 5$, the following holds:

$$D_0 = -\frac{p_0 - 1}{2}, K_0 = -\frac{p_0 + 1}{2} \tag{2.14}$$

According to (12) and (13), a recurrence relation is derived for $\{p_k\}$, where

$$p_k = \left(\frac{p_{k-1} - 1}{2}\right)^2 + \left(\frac{p_{k-1} + 1}{2}\right)^2 = \frac{p_{k-1}^2 + 1}{2} \tag{2.15}$$

In (14), picking $p_0 = 61$, we calculate the first three terms of the series $\{p_k\}, k = 1, 2, 3, ...$, as follows:

$$p_1 = \left(\frac{p_0 - 1}{2}\right)^2 + \left(\frac{p_0 + 1}{2}\right)^2 = 30^2 + 31^2 = 1861 = 60 \cdot 31 + 1 = 60\ \frac{p_0 + 1}{2} + 1\,,$$

$$p_2 = \left(\frac{p_1 - 1}{2}\right)^2 + \left(\frac{p_1 + 1}{2}\right)^2 = 930^2 + 931^2 = 1731661 = 60 \cdot 31 \cdot 931 + 1 = 60\ \frac{p_0 + 1}{2}\ \frac{p_1 + 1}{2} + 1\,,$$

$$p_3 = \left(\frac{p_2 - 1}{2}\right)^2 + \left(\frac{p_2 + 1}{2}\right)^2 = 865830^2 + 865831^2 = 1499324909461 = 60\ \frac{p_0 + 1}{2}\ \frac{p_1 + 1}{2}\ \frac{p_2 + 1}{2} + 1\,,$$

$$\vdots$$

$$p_k = \left(\frac{p_{k-1} - 1}{2}\right)^2 + \left(\frac{p_{k-1} + 1}{2}\right)^2 = 60 \prod_{i=0}^{k-1} \frac{p_i + 1}{2} + 1 = \left(60 \prod_{i=0}^{k-2} \frac{p_i + 1}{2}\right) \frac{p_{k-1} + 1}{2} + 1 = A\ \frac{p_{k-1} + 1}{2} + 1\,. \tag{2.16}$$

According to (15), the value A has the form:

$$A = 60 \prod_{i=0}^{k-2} \frac{p_i + 1}{2} \tag{2.17}$$

Considering (15), (16) and (17), we obtain an equation for p_{k-1} :

$$A\ \frac{p_{k-1} + 1}{2} + 1 = \frac{p_{k-1}^2 + 1}{2}$$
$$p_{k-1}^2 - A\ p_{k-1} - A - 1 = 0 \tag{2.18}$$

Solving the equation (16), we obtain the term p_{k-1} in the series $\{p_k\}$:

$$p_{k-1} = A + 1 \tag{2.19}$$

According (16) and (18), we have:

$$p_{k-1} = 60 \prod_{i=0}^{k-2} \frac{p_i + 1}{2} + 1 \tag{2.20}$$

Using Euler's formula, $x^2 + y^2 = N$, and choosing an appropriate form for [6], it was shown that the obtained numbers, $p_1,\ p_2,\ p_3$ are prime. The primality of the first three terms, also the fact that the series $\{p_i\}$ has direct (15) and inverse (19) recurrences implies that this series is composed of infinite number of primes of the form $p_i = 60m_i + 1$. According to Definition 10, this evidences the existence of the infinite number of indivisible lines in the discrete metric space $\aleph(D)$ (10), which in own turn, stand for prime numbers' separate series generators.

3. Efficiency of Generating Primes in the Space of Discrete Geometries vs. Testing for Primality

Development of Information security and assurance algorithms point out to the need of selecting one or more very large primes at random [12]. Prime numbers are applied in areas of computer games, software testing, hashing algorithms, and also in lots of mathematical programming tools, which perform arithmetic on large integers or polynomials applying reductions modulo primes. In the RSA cryptosystem all arithmetic is done modulo n, with $n = pq$ and p, q large primes. Decryption in this system relies on computing Euler's phi function, $\varphi(n)$, which is hard to compute, and hence the system is hard to break, unless one knows the prime factorization of n.

Up to date, the respective software designers are faced the task of determining whether a given large number is prime. There is no simple yet efficient means of accomplishing this task, not to mention the possibility of generating a prime number of the required order.

The existing Prime Numbers Generators and Checkers support the following operations on natural numbers: Checking - prime number checker determines if the given number is a prime; Finding next - prime number generator finds the smallest prime number greater than the provided number; Find previous - prime number generator finds the largest prime number smaller than the given number.

Another issue in prime numbers generation is how many numbers are likely to be rejected before a prime number is found. A result from number theory, known as the prime number theorem, states that the primes near N are spaced on the average one every $(\ln(N))$ integers. Thus, on average, one would have to test on the order of $\ln(N)$ integers before a prime is found.

A variety of tests for primality have been developed, and almost invariably, the tests are probabilistic. That is, the test will merely determine that a given integer is probably prime. In one of the more efficient and popular algorithms, the Miller-Rabin algorithm [13], and several others [14, 15, 16], the procedure for testing whether a given integer n is prime is to perform some calculation that involves n and a randomly chosen integer a. If n "fails" the test, then n is not prime. If n "passes" the test, then n may be prime or nonprime. If n passes many such tests with many different randomly chosen values for a, then we can have high confidence that n is, in fact, prime.

The sieve-based algorithms are the most efficient algorithms currently known for generating prime numbers [17, 18, 19]. Time complexity of calculating all primes below n in the random access machine model is $O(nlog\ logn)$ operations, a direct consequence of the fact that the prime harmonic series asymptotically approaches $log\ logn$. It has an exponential time complexity with regard to input size, though, which makes it a pseudo-polynomial algorithm.

The formulas derived in (16) and (19) evidence the existence of prime numbers' efficient recursive generation

in the space of discrete geometries, and exhibits a polynomial time complexity in generating the primes in the series.

4. Conclusion

A recursive generation of prime numbers is introduced based on stratification of the discrete geometrical space into subspaces, where to each subspace an individual indivisible line is associated. The indivisible lines together with the prime numbers are of geometrical and arithmetical significance and content in the space $\aleph(D)$ due to their unique complex of properties and peculiarities, namely, discreteness, infinity, asymmetry, non-homogeneousness, null-dimensions and quantized character.

References

[1] Yu. G. Grigoryan, *Principles of inhomogenous geometry*, J. Algebra, Geometry and their Applications, **3-4** (2004), 40-53.

[2] Yu. G. Grigoryan, *Discrete geometric space*, Cybernetics and Systems Analyses **42** (2006), 631-640.

[3] Yu. G. Grigoryan, *Nonclassical properties of a discrete geometries space*, Cybernetics and Systems Analysis **45** (2009), 714-722.

[4] A. N. Vyaltsev, *Discrete Space-Time*,(in Russian), KomKniga, Moscow, 2007.

[5] Yu. G. Grigoryan, *Indivisible lines in the space of discrete geometries*, IEEE Conference Publications: Computer Science and Information Technologies(CSIT) (2013), 1-4.

[6] Yu. G. Grigoryan, *Asymmetry and kernel of the coded metric space*, J. Mathematical Problems Computer Science, (in Russian) **38** (2012),10-11.

[7] Yu. G. Grigoryan, *The variational problem of functions of logical algebra and a method for its computer realization*, Cybernetics and Systems Analysis **3** (1967), 21-24.

[8] Yu. G. Grigoryan, *Existence and representation of natural arithmetic graphs*, USSR Computational Mathematics and Mathematical Physics **24** (1984), 100-103.

[9] Yu. G. Grigoryan, *Arithmetic automorphism group of simple cycles*, Cybernetics and Systems Analyses 26 (1990), 464-475.

[10] Yu. G. Grigoryan, *Discrete geometries space*, Cybernetics and Systems Analyses **4** (1982), 403-406.

[11] Yu. G. Grigoryan, G.K. Manoyan, *Certain questions of the arithmetical interpretation of nonoriented graphs*, Cybernetics and Systems Analysis **13** (1977), 448-451.

[12] W. Diffie, M. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory IT **22** (1976), 644-654.

[13] G. L. Miller, *Riemann's hypothesis and tests for primality*. Proc. Seventh Annual ACM Symp. on the Theory of Computing. Albuquerque, New Mex. (1975), 234-239.

[14] J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Camb. Phil. Soc. 76 (1974) 521-528.

[15] R. Solovay, V. Strassen, *A Fast Monte-Carlo test for primality*, SIAM Journ. Comput. **6** (1977), 84-85.

[16] D. E. Knuth, *The Art of Computer Programming, Vol 2: Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969.

[17] L. Xuedong, *A practical sieve algorithm finding prime numbers*, Communications of the ACM **32** (1989), 344-346

[18] S. H. Bokhari, *Multiprocessing the sieve of Eratosthenes*, IEEE Computers, **20** (1987), 50-58.

[19] R. Crandall, C. Pomerance. *Prime Numbers, a Computational perspective*, Springer-verlag, 2001.