Analysis of Algorithms (AofA):

Wojciech Szpankowski*
Department of Computer Science
Purdue University
W. Lafayette, IN 47907
U.S.A.

Abstract
This is the first installment of the Algorithmics Column dedicated to Analysis of Algorithms (AofA) that sometimes goes under the name Average-Case Analysis of Algorithms or Mathematical Analysis of Algorithms. The area of analysis of algorithms (at least, the way we understand it here) was born on July 27, 1963, when D. E. Knuth wrote his “Notes on Open Addressing”. Since 1963 the field has been undergoing substantial changes. We report here how it evolved since then. For a long time this area of research did not have a real “home”. But in 1993 the first seminar entirely devoted to analysis of algorithms took place in Dagstuhl, Germany. Since then seven seminars were organized, and in this column we briefly summarize the first three meetings held in Schloss Dagstuhl (thus “Dagstuhl Period”) and discuss various scientific activities that took place, describing some research problems, solutions, and open problems discussed during these meetings. In addition, we describe three special issues dedicated to these meetings.

1 Introduction
The area of analysis of algorithms was born on July 27, 1963, when D. E. Knuth wrote his “Notes on Open Addressing” about hashing tables with linear probing (cf. Knuth’s notes http://pauillac.inria.fr/algo/AofA/Research/src/knuth1rait-bwd.gif). The electronic journal Discrete Mathematics and Theoretical Computer Science (cf. the website http://dmtcs.loria.fr/) defines this area as follows:

Analysis of Algorithms is concerned with accurate estimates of complexity parameters of algorithms and aims at predicting the behaviour of a given algorithm run in a given environment. It develops general methods for obtaining closed-form formulae, asymptotic estimates, and probability distributions for combinatorial or probabilistic quantities, that are of interest in the optimization of algorithms. Interest is also placed on the methods themselves, whether combinatorial, probabilistic, or analytic. Combinatorial and statistical properties of discrete structures (strings, trees, tries, dags, graphs, and so on) as well as mathematical objects (e.g., continued fractions, polynomials, operators) that are relevant to the design of efficient algorithms are investigated.

*This research was supported in part by the NSF Grants CCR-9804760 and CCR-0208709, and Purdue Faculty Grant GHFC-9919.
In fact, the name “analysis of algorithms” did not emerge easily. D. E. Knuth, the founder of the area, in the abstract of his talk “The Birth of the Giant Component” [16, 31] given during the first Average Case Analysis of Algorithms Seminar, Dagstuhl, July 12 – 16, 1993 has the following to say:

The first few minutes of this talk considered “the birth of analysis of algorithms” – my personal experiences from 31 years ago when I first noticed how pleasant it is to find quantitative formulas that explain the performance characteristics of important algorithms. Those experiences profoundly changed my life! I also mentioned why it became necessary to invent a name for such activities.

We finally settled on “Analysis of Algorithms” after considering “Precise Analysis of Algorithms”, “Mathematical Analysis of Algorithms”, and “Average-Case Analysis of Algorithms”.

Since its inception in 1963 the field has been undergoing substantial changes. We see now the emergence of combinatorial and asymptotic methods that allow the classification of data structures into broad categories that are amenable to a unified treatment. Probabilistic methods [2, 63] that have been so successful in the study of random graphs [3] and hard combinatorial optimization problems play an equally important role in this field. These developments have two important consequences for the analysis of algorithms: it becomes possible to predict average behavior under more general probabilistic models [45, 59, 63]; at the same time it becomes possible to analyze much more structurally complex algorithms [20, 23, 26, 27, 28, 29, 31, 32, 33, 34, 42, 37, 38, 39, 41, 43, 44, 51, 55, 56, 57, 62, 64, 66]. To achieve these goals the analysis of algorithms draws on a number of branches in mathematics: combinatorics, probability theory, graph theory, real and complex analysis, number theory and occasionally algebra, geometry, operations research, and so forth.

This is the first column on the analysis of algorithms. Our goal is to describe some activities in this area since 1993 when the first workshop on analysis of algorithms took place. We briefly describe the first three seminars, outlining some presentations and discussing in depth some results published in three post-conference special issues. In the forthcoming paper (Part II) we shall report about activities after 1998.

2 Average-Case Analysis of Algorithms, Dagstuhl, 1993

In 1990 during the Random Graphs conference in Poznań Philippe Flajolet, Rainer Kemp and Helmut Prodinger decided to organize a seminar exclusively devoted to analysis of algorithms. Such a workshop took place in Dagstuhl, July 12 – July 16, 1993 with over thirty participants, including the founder of the area, D. E. Knuth. The organizers summarized this meeting in the Dagstuhl Seminar Report [16], where one finds the following quote:

This meeting was the first one ever to be dedicated exclusively to analysis of algorithms. The number of invited participants was 37, of which 30 gave presentations of recent results summarized below. The talks could be grouped roughly as dealing with Methods or Applications, both aspects being often closely intertwined.
Methods were well represented during the seminar. Actually, the first talk by D. E. Knuth on evolution of random graphs belongs to this category. This talk was the highlight of the conference, and we dwell a little bit on it. Knuth’s presentation was based on an over hundred page paper [31] published in Random Structures & Algorithms co-authored by S. Janson, T. Łuczak, and B. Pittel. (In a sense, this paper is a continuation of the work by Flajolet, Knuth and Pittel [20] where analytic tools were used to study the first cycles in random graphs.) The principal result of Knuth’s paper is that an evolving graph or multigraph on \( n \) vertices has at most one component through its evolution with probability \( \frac{25n}{18} \approx 0.8727 \) as \( n \to \infty \). This result is obtained by analytic tools of generating functions and their functional/differential equations. For example, Knuth proves that the generating function \( G(w, z) \) for random multigraphs satisfies

\[
G(w, z) = e^z + \frac{1}{2} \int_0^\infty \vartheta^2 G(w, z) dw
\]

where \( \vartheta \) is the operator \( z \frac{\partial}{\partial z} \). Enumeration of this sort, together with counting trees, unicycle components and bicyclic components in random graphs are analyzed in Knuth’s paper.

Throughout the presentation Knuth refers to the tree function defined as

\[
T(z) = ze^{T(z)}
\]

from which, by Lagrange’s inversion formula, we find

\[
[z^n] T(z) = \frac{n^{n-1}}{n!}.
\]

In the sequel, we shall use the standard notation \([z^n] F(z)\) for the coefficient at \( z^n \) of the power series \( F(z) \). Of course, \( T(z) \) generates rooted labeled trees, but it arises in surprisingly many applications; it will appear many times in this article. As a matter of fact, it was generalized by Knuth and Pittel in [42] as well as in [31]. Let

\[
B(z, y) = \frac{1}{(1 - T(z))^y} = \sum_{n=0}^\infty t_n(y) \frac{z^n}{n!},
\]

where \( t_n(y) \) is a polynomial of degree \( n \) in \( y \), called the tree polynomial of order \( n \). In particular,

\[
t_n(1) = n^n.
\]

Furthermore, \( t_n(2) = n^n(1 + Q(n)) \)

where

\[
Q(n) = \sum_{k=1}^{n-1} \frac{n!}{(n-k)!k^k}
\]

is the Ramanujan function studied in 1962 by Knuth and denoted by him as \( Q \). Related identities and functions appear in an incredible number of analyses: caching, hashing and birthday paradox, random number generators and integer factorization (by Pollard’s rho method), and union-find algorithms. Lately, they were even used in source and channel coding (cf. [24, 61, 62]).
To finish our discussion about Knuth’s presentation, let us mention that another speaker of the seminar, K. Compton, talked about “Ramanujan’s $Q$-function and Asymptotics” and its applications to an analysis of a multiprocessing systems [7].

There were many other presentations in the Methods category. We mention here “The Mellin Transform Technology” by P. Flajolet and “Ramanujan and the Average Case Analysis of Trie Parameters” by Kirschenhofer and Prodinger. The first presentation found its way to the special issue of Theoretical Computer Science that was published in 1995.

Applications group was also well represented. Sedgewick talked about his and Schaffer’s solution of a 20 years old problem concerning the average-case analysis of heapsort [57]. Vallée demonstrated how the lattice reduction algorithm of Gauss can be precisely analyzed. Finally, there were three talks related to the behavior of data compression (Jacquet, Szpankowski, Vitter). For the first time a precise analysis of the Lempel-Ziv compression scheme was presented (we shall discuss it below in some depth).

During the seminar several open problems were discussed; ten of them were recorded in the Dagstuhl Report [16]. We describe here only one that initiated a long term project by Michael Drmota (see also Reed [54]) who solved it finally in 2000 [13, 14]. (We come back to it in Part II when we discuss the 2000 post-conference special issue.) The problem was posed by P. Flajolet and we quote here from [16]:

Luc Devroye [10] (cf. also [11]) has used probabilistic arguments to show that the expected height of a random binary search tree over $n$ nodes is asymptotic to $c \log n$, where $c$ is Robson’s constant ($c \approx 4.3$). The problem can be recast in analytic terms as follows: Let

$$y_{h+1}(z) = 1 + \int_0^z y_h^2(t)dt, \quad y_0(z) = 0,$$

(3)

(so that $y_{\infty}(z) = \frac{1}{1-z}$). Then the generating function of average heights

$$H(z) = \sum_{h=0}^{\infty} [y_{\infty}(z) - y_h(z)]$$

(4)

satisfies

$$H(z) \sim \frac{c}{1 - z} \log \frac{1}{1 - z}, \quad z \to 1.$$

(5)

The problem is to show this estimate in an extended area of the complex plane. Devroye’s result follows from (5). A consequence of an analytic proof of (5) should be to derive estimates on the variance (the exact order is yet unknown) of height, and most probably also a limiting distribution result.

It turned out that one needs more terms in (5) to obtain the conjectured results concerning the variance and the limiting distribution. Indeed, the expected value of the height followed from (5), as proved by Drmota [13], however, for the variance (which turns out to be bounded) Drmota [14] and Reed [54] needed more terms of the asymptotic expansion of the height plus additional concentration properties. The limiting distribution is not yet proved rigorously, however, a heuristic argument based on the WKB method was recently presented in [36].
In 1995 H. Prodinger and W. Szpankowski edited a special issue entitled “Mathematical Analysis of Algorithms” in *Theoretical Computer Science*, 144, No. 1-2. It was dedicated to D. E. Knuth, the founding father of the area. This special issue was meant to be a post-Dagstuhl-seminar collection of results, however, we advertised it in an open call for papers. We accepted 10 papers and Philippe Flajolet wrote an invited paper that we discuss in some depth below, together with a few others.

In the invited paper [19] Flajolet and his colleagues X. Gourdon and P. Dumas present a unified and essentially self-contained approach to the Mellin transform. The Mellin transform (Hjalmar Mellin 1854–1933, Finish mathematician) is the most popular transform in analysis of algorithms. It is defined for a real-valued function \( f(x) \) on \((0, \infty)\) as

\[
f^*(s) = \int_0^\infty f(x)x^{-s}dx
\]

provided the above integral exists, with \( s \) being a complex number. D. E. Knuth, together with De Bruijn, introduced it in the orbit of discrete mathematics in the mid-1960s, however, Flajolet’s school systematized and applied the Mellin transform to myriad problems of analytic combinatorics and analysis of algorithms. The popularity of this transform stems from two important properties. It allows the reduction of certain functional equations to algebraic ones, and it provides a direct mapping between asymptotic expansions of a function near zero or infinity and the set of singularities of the transform in the complex plane (cf. Table 1).

In analysis of algorithms and analytic combinatorics one often deals with functional equations like

\[
f(x) = a(x) + \alpha f(xp) + \beta f(xq), \tag{6}
\]

where \( \alpha, \beta \) are constants, and \( a(x) \) is a known function (e.g. think of the divide-and-conquer recursion or splitting processes). The Mellin transform maps the above functional equation into an algebraic one that is easier to solve and hence allows us to recover \( f(x) \), at least asymptotically as \( x \to 0 \) or \( x \to \infty \) (cf. property (M4) in Table 1). Indeed, the Mellin transform of \( f(x) \) defined in (6) is

\[
f^*(s) = a^*(s) + \alpha p^{-s}f^*(s) + \beta q^{-s}f^*(s)
\]

provided there is a strip in the complex plane where \( f^*(s) \) exists.

Flajolet and his colleagues concentrate in [19] on sums like

\[
G(x) = \sum_{k=0}^\infty \left(1-e^{-x/2^{k}}\right) \quad \text{and} \quad H(x) = \sum_{k=1}^\infty (-1)^k e^{-k^2 x}\log k,
\]

which are typical examples of a harmonic sum

\[
\sum_k a_k f(b_k x)
\]

whose Mellin transform becomes (cf. property (M3) in Table 1)

\[
\sum_k a_k b_k^{-s} f^*(s).
\]
(M1) Direct and Inverse Mellin Transforms. Let \( c \) belong to the fundamental strip defined below.

\[
f^*(s) := \mathcal{M}(f(x); s) = \int_0^\infty f(x)x^{s-1}dx \quad \iff \quad f(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} f^*(s)x^{-s}ds. \tag{7}
\]

(M2) Fundamental Strip. The Mellin transform of \( f(x) \) exists in the fundamental strip \( \Re(s) \in (-\alpha, -\beta) \), where

\[
f(x) = O(x^\alpha) \quad (x \to 0), \quad f(x) = O(x^\beta) \quad (x \to \infty)
\]

for \( \beta < \alpha \).

(M3) Harmonic Sum Property. By linearity and the scale rule \( \mathcal{M}(f(ax); s) = a^{-\mu} \mathcal{M}(f(x); s) \),

\[
f(x) = \sum_{k \geq 0} \lambda_k g(\mu_k x) \quad \iff \quad f^*(s) = g^*(s) \sum_{k \geq 0} \lambda_k \mu_k^{-s}. \tag{8}
\]

(M4) Mapping Properties (Asymptotic expansion of \( f(x) \) and singularities of \( f^*(s) \)).

\[
f(x) = \sum_{(\xi, k) \in A} c_{\xi, k} x^\xi (\log x)^k + O(x^M) \quad \iff \quad f^*(s) \asymp \sum_{(\xi, k) \in A} c_{\xi, k} \frac{(-1)^k k!}{(s+\xi)^{k+1}}. \tag{9}
\]

— (i) Direct Mapping. Assume that \( f(x) \) admits as \( x \to 0^+ \) the asymptotic expansion (9) for some \( -M < -\alpha \) and \( k > 0 \). Then for \( \Re(s) \in (-M, -\beta) \), the transform \( f^*(s) \) satisfies the singular expansion (9)

— (ii) Converse Mapping. Assume that \( f^*(s) = O(|s|^{-r}) \) with \( r > 1 \), as \( |s| \to \infty \) and that \( f^*(s) \) admits the singular expansion (9) for \( \Re(s) \in (-M, -\beta) \). Then \( f(x) \) satisfies the asymptotic expansion (9) at \( x = 0^+ \).

Table 1: Main Properties of the Mellin Transform.

From the inversion formula of the Mellin transform one obtains (cf. property (M1) in Table 1)

\[
\sum_k a_k f(b_k x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \sum_k a_k b_k^{-s} f^*(s)x^{-s}ds.
\]

Shifting the line of integration and collecting all residues leads to the desired asymptotics of the harmonic sum. This basic Mellin transform formula for harmonic sum is the starting point for Flajolet and his colleagues to a readable account on Mellin transform and its application to analysis of algorithms (cf. also [22, 45, 63]). For a summary of Mellin transform properties the reader may consult Table 1.

Finally, we say a few words about the Jacquet and Szpankowski paper [28] that appeared in the same special issue. It was devoted to the analysis of the Lempel-Ziv’78 data compression scheme, and its relation to digital search trees. This scheme partitions a sequence of
length \( n \) into variable phrases such that a new phrase is the shortest substring not seen in the past as a phrase. The parameter of interest is the number \( M_n \) of phrases that one can construct from a sequence of length \( n \). Its behavior determines the compression ratio of this scheme. It was known that for stationary and ergodic sources

\[
M_n \sim \frac{nh}{\log n}, \quad \text{(a.s.)}
\]

where \( h \) is the entropy of the source. However, to gain more insights (e.g., to compute the average redundancy of the code as in [44]) one needs more refined information about \( M_n \). In particular, Ziv asked in 1978 about the limiting distribution of \( M_n \) conjecturing that it must be normal. Aldous and Shields [1] solved the problem for memoryless unbiased sources (i.e., each symbol is generated by the same probability independently of others), however, the authors of [1] insisted that “... we are not optimistic about finding a general result. We believe the difficulty of our normality result is intrinsic ...”. In fact, the authors of [1] were not able to estimate precisely the variance due to some oscillation. The problem of variance was solved by Kirschenhofer, Prodinger, and Szpankowski [34], still for unbiased memoryless sources. Jacquet and Szpankowski set out to extend Aldous and Shields results to biased memoryless sources. Not surprisingly, the method used by the authors of [28] was mostly analytic, but with a help from probabilistic methods (e.g., Billingsley’s renewal lemma) needed to translate analytic results obtained for digital search trees to limiting distribution of the Lempel-Ziv scheme.

As mentioned above, the problem is reduced to finding the limiting distribution of the total path length in a digital search tree built from independently generated strings. Let \( L(z, u) \) be the bivariate probability generating function of the path length in the Poisson model in which the fixed number of strings is replaced by a random number of strings generated according to the Poisson distribution. It satisfies the following differential-functional equation

\[
\frac{\partial L(z, u)}{\partial z} = L(pzu, u)L(qzu, u)
\]

with \( L(z, 0) = 1 \), where \( p \) (\( q = 1 - p \)) is the probability of generating a “0”. Usually, the Poisson model is easier to solve than the original Bernoulli model, but is far from being trivial. In fact, it is known only how to obtain asymptotic results for the Poisson model for \( z \to \infty \) in a cone. Once it is proved that \( \log L(z, u) = \Theta(z^{\kappa(u)}) \) for some function \( \kappa(u) \) in a cone around the real axis (and all derivatives of \( L(z, u) \) with respect to \( u \) are proved to be bounded), the Poisson model can be asymptotically solved. Then the authors of [28] “wrestle” with a particularly complicated depoissonization in order to translate the Poisson model back to the the Bernoulli model (for a more detailed exposition of analytic depoissonization the reader is referred to [29]). The final outcome of this tour de force is a pretty complete analysis of the limiting distribution and well as the first two moments. The authors of [28] propose also a large deviation result, however, the exact exponent is not determined (and is still an open problem; see Conjecture 1 below).

Actually, we finish this section with an open problem regarding the analysis of the Lempel-Ziv scheme for a Markovian source. We formulate it as a conjecture.
**Conjecture 1** Consider a (stationary, irreducible and aperiodic) Markovian source with transition probabilities \{p_{ij}\}_{i,j=1}^n. Set \(\Lambda(x) = \frac{H}{H} \log x - \frac{H}{H} x + O(\log x)\) where \(A = \gamma - 1 + \lambda(-1) + \frac{\lambda(-1)}{2} - \vartheta - \pi_s(-1) + \delta_1(\ln m)\) with \(\lambda(s)\) and \(\lambda_l(s)\) are the first and the second derivative of the eigenvector \(\lambda(s)\) of \(P(s) = \{p_{ij}^{-1}\}_{i,j=1}^n\), while \(\vartheta\) is a constant that we can explicitly compute. Define \(x_n\) as a solution of \(\Lambda(x_n) = n\), that is,

\[
x_n = \frac{\frac{H}{H} \log n }{\log n} \left(1 + \frac{\log \log n}{\log n} + \frac{A - \log H}{\log n} + O \left( \frac{(\log \log n)^2}{\log^2 n} \right) \right).
\]

Then

\[
\mathbb{E} M_n^k = x_n^k \left(1 + O \left( \sqrt{\frac{\log n}{n}} \right) \right) + O \left( \frac{n^{k-1}}{\log^{k-1} n} \right)
\]

\[
\text{Var} M_n \sim \frac{c_2 H^3 n}{\log^2 n} + O(1),
\]

\[
\frac{M_n - \mathbb{E} M_n}{\sqrt{\text{Var} M_n}} \to N(0,1),
\]

\[
\lim_{n \to \infty} \frac{1}{n} \log \Pr \left\{ M_n > \Lambda^{-1} \left( \frac{n}{1-y} \right) \right\} = -\frac{I(y)}{1-y}
\]

where \(0 < y < 1\) and \(I(y)\) is a function (at this point we still do not know how to compute this function). Moreover, moments of \(M_n\) converge to the appropriate moments of the normal distribution.

The above formulas, except (15), are natural extensions of [28] and recent results presented in [30] concerning the Lempel-Ziv phrase distribution for Markov sources. The large deviation result (15) is not even proved for memoryless sources, however, based on known large deviation results for other codes (cf. [49]) we expect this formula to be true (provided one finds an expression for the exponent \(I(y)\)).

# 3 Average-Case Analysis of Algorithms, Dagstuhl, 1995

The second *Average-Case Analysis of Algorithms* seminar took place in Dagstuhl, July 3-7, 1995. It was organized by P. Flajolet, R. Kemp, H. Prodinger, and R. Sedgewick. In the post-conference abstract [17] the organizers have the following to say:

The field is undergoing tangible changes. We see now the emergence of combinatorial and asymptotic methods that permit to classify data models into broad categories that are susceptible of unified treatment. This has two important consequences for the analysis of algorithms: it becomes possible to predict average-case behavior of more complex data models (for instance, nonuniform models and even Markovian dependencies); at the same time it becomes possible to analyze much more structurally complex algorithms since we have a much higher level grasp on the average-case analysis process.
On the analytic side, there were talks on diagonal Poisson transform (Viola [29]) and analytic deconvolution (Jacquet and Szankowski [29]). These tools of general nature are strongly tied with the analysis of hashing and digital trees or data compression. Tools for extracting limiting distributions were discussed by Drmota and Szpankowski [29].

In Dijkstra's 1969, there were a few talks on trees and their analyses (Flajolet, Hulbeck, Gittenberger, Prodinger, Steyer). For example, in an interesting paper [32], Solution of a Problem of Yekutieli and Mandelbrot. H. Prodinger solved an open problem posed by Yekutieli and Mandelbrot asking the larger of the two. "If the tree has register function, then the whole tree must be assigned the larger order number."

While this rule is defined recursively as follows: leaves get the lower order number equal to 0, while a left child is defined as 1. Using generating functions, Melan transformations and singularity value oscillates between 3 and 4. Using generating functions, Melan transformations and singularity value oscillates between 3 and 4.

Lastly, there were a few talks on new applications of analysis of algorithms. M. Regnier, presented a talk on the parallel implementation of the Karanbakh's algorithm. R. A. Wright, an expert in the field, gave a talk about the different methods used to analyze algorithms. Finally, R. A. Wright spoke about parallel scheduling.
an analytic solution \( y(x, z) \) of the following (system of) functional equation(s)

\[
y = F(x, y, z).
\]

Examples of such equations are:

\[
y(x, z) = xz + \frac{xy(x, z)}{1 - y(x, z)}
\]

that represents the number of planted plane trees with given number of leaves; and

\[
y(x, z) = \frac{x}{1 - y(x, z)} - xy(x, z)^d + xzy(x, z)^d
\]

which is the generating function for the numbers \( y_{n,k} \) of planted plane trees of size \( n \) and \( k \) nodes of outdegree \( d \). Drmota reduces the analysis of (16) to the following form

\[
y(x, z) = g(x, z) - h(x, z)\sqrt{1 - x/f(z)}
\]

with proper analytic functions \( g(x, z) \), \( h(x, z) \), and \( f(z) \). This form is a consequence of the Weierstrass preparation theorem. In the next step Drmota applied the Flajolet and Odlyzko [21] transfer theorem to obtain the asymptotics of \( y_n(z) = [x^n]y(x, z) \). Finally, the saddle point method applied to the Cauchy formula completed the derivations.

In summary, Drmota proves that the coefficient (we deal here only with the one-dimensional case) of

\[
y(x, z) = \sum_{n,m} y_{n,m} x^n z^m
\]

has the following asymptotic solution

\[
y_{n,m} = \frac{a x_0^{-m}}{2\pi n^2 \sqrt{2\pi}} \exp\left(\frac{(m - \mu n)^2}{2n \sigma^2}\right) + O(n^{-1/2})
\]

where \( a, x_0, \mu \) and \( \sigma \) are certain constants. In the multidimensional case one obtains a similar expansion. The above formula is an example of a local limit Gaussian approximation.

4 Average-Case Analysis of Algorithms, Dagstuhl, 1997

The third Average-Case Analysis of Algorithms seminar took place in Dagstuhl, July 7-11, 1997. It was organized by P. Flajolet, R. Kemp, H. Mahmoud, and H. Prodinger. Twenty eight talks were given ranging from methodological to applied, covering such diverse problems as string matching and computational biology, hashing, tree data structures, selection problems in statistics, data compression and information-theory, adaptive data structures and learning, real-time and system programming, as well as computer algebra. We discuss some of them below.

Urn models were presented by Gardy who stressed their diverse applications to hashing, allocations or learning. Guy Louchard, a pioneer of the Brownian motion approach to analysis of algorithms (cf. [43]) used Brownian excursion local times to the analysis of random trees,
while Luc Devroye presented a unifying approach to the analysis of depth and height for random search trees.

Analytic combinatorics were well represented in talks of Flajolet (on Gaussian laws), Odlyzko (on constrained set partitions) and Salvy (on automatic saddle point methods).

Pattern in strings are of interest to a number of applications such as retrieval, indexing, computational biology, source coding, and so forth. Several talks were devoted to this topic. Régnier presented a generalization of the Guibas and Odlyzko “autocorrelation” to sequences generated by Markovian sources (cf. [55]). Nebel applied formal languages to an interesting enumerative problem on strings. Vallée used dynamic systems approach to analyze digital tree for the so called dynamic sources (cf. [65]).

As expected, trees have attracted a lot of interest from AofA community, however, combinatorial models still pose intriguing questions. Kemp analyzed balanced trees. Drmota had the first “crack” into the problem of height in a binary search tree using analytic approach, as suggested by Flajolet during the first Dagstuhl meeting. Mahmoud gave a solution to the quickselect algorithm, which can be viewed as a one-sided quicksort (a complete analysis of the regular quicksort problem is still needed). Finally, Bob Sedgewick surveyed some sixty open problems introduced by Knuth in his Vol. 3 and discussed about twenty of them that were solved. Three open problems were discussed in detail, namely the average case analysis of shellsort, balanced trees, and development of sorting networks that are substantially better than Batcher’s network.

In passing, we should mention that there were several talks illustrating applications of analysis of algorithms. Golin focused on computational geometry, Fill discussed self-organizing search, Coffman gave a talk on reservation policies in communication systems (cf. [6], Jacquet analyzed an on/off queue, and Schmid surveyed some recent results in real-time systems (cf. [58]).

We end this brief presentation with the highlight of the Dagstuhl 1997 meeting, namely a definite solution to the variance analysis of linear probing hashing that was presented for the first time by Poblete and Viola. This unfolding story has it continuation in the special issue that we discuss next.

Following our tradition, we edited a special issue of Algorithmica, vol. 22, No. 2, 1998 (eds. H. Prodinger and W. Szpankowski), where we collected more definite results presented during the last AofA meeting. This was very “special” special issue. It was dedicated to “…our colleague, teacher, and friend Philippe Flajolet on the occasion of his 50th birthday”. The editors prepared an article on “Philippe Flajolet’s Research in Analysis of Algorithms” [53] describing Flajolet’s accomplishments in analysis of algorithms.

In my opinion this special issue was one of the best so far devoted to analysis of algorithms that I was involved in. A number of research results were published that solved long standing open problems. In particular, we dwell on two results, namely that of linear probing hashing by Flajolet, Poblete, Viola [23] and Knuth [40], and (in Knuth’s words) “an exciting paper” [64] by Vallée who for the first time analyzed rigorously the binary Euclidean gcd algorithm proving a 20-year old conjecture of Brent.

Let us recall that in linear probing hashing a table of length \( m \) is set up together with a hash function \( h \) that maps \( n \leq m \) keys (randomly) to the \( m \) cells of the hash table. A
collection of \( n \) objects (keys) enter sequentially into the hash table so that element \( x \) is placed at the first unoccupied location starting from \( h(x) \) in a cyclic order. The displacement is the number of collisions until an unoccupied cell is found. The total displacement corresponding to a sequence of hashed values is the sum of all individual displacement, and it is usually denoted as \( d_{m,n} \). In his 1963 paper Knuth proved that

\[
\mathbb{E}[d_{m,n}] = \frac{n}{2}(Q_0(m, n - 1) - 1) \tag{17}
\]

where \( Q_r(m, n) \) is the generalized Ramanujan’s function defined as

\[
Q_r(m, n) = \sum_{k \geq 0} \binom{r + k}{k} \frac{n^{n-1}}{m^{n-k+1}}.
\]

Here are Knuth’s personal remarks from [40] regarding this problem:

The problem of linear probing is near and dear to my heart, because I found it immensely satisfying to deduce (17) when I first studied the problem is 1962. Linear probing was the first algorithm that I was able to analyze successfully, and the experience had a significant effect on my future career as a computer scientist. None of the methods available in 1962 were powerful enough to deduce the expected square displacement, much less the higher moments, so it is an even greater pleasure to be able to derive such results today from other work that has enriched the field of combinatorial mathematics during a period of 35 years.

We end up this essay with a pretty detailed description of the derivation that Knuth was able to carry on after 35 years. In fact, we follow Knuth as well as Flajolet, Poblete and Viola [23] whose analysis lead to a distribution of the total displacement.

The most interesting behavior of linear probing hashing occurs when \( m = n \) or \( m = n - 1 \) which we shall call full and almost full tables, respectively. Here, we only consider the case when \( n = m - 1 \) and write \( d_n = d_{n,n-1} \). Using Knuth’s circular symmetry argument we shall assume from now on that the nonempty cell is the rightmost one. Define \( F_{n,k} \) as the number of ways of creating an almost full table with \( n \) elements (with empty cell in the rightmost location) and total displacement \( k \). The bivariate generating function is denoted as

\[
F(z, u) = \sum_{n,k \geq 0} F_{n,k} u^k \frac{z^n}{n!}.
\]

Following Knuth [40], and Flajolet, Poblete and Viola [23] we observe that \( F_n(u) = n! \left[ z^n \right] F(z, u) \) satisfies

\[
F_n(u) = \sum_{k=0}^{n-1} \binom{n-1}{k} F_k(u)(1 + u + \cdots + u^k)F_{n-1-k}(u).
\]

Indeed, consider an almost full table of size \( n \) (and length \( n + 1 \) with the rightmost location empty). Just before the last element is inserted there is another empty cell, say at position \( k + 1 \). The address of the last element belongs to the interval \([1..k+1]\) which corresponds to the displacement in the interval \([0..k]\). The above functional equation follows. Observe
also that after some simple algebra this equation satisfies the following differential-functional equation

\[
\frac{\partial}{\partial z} F(z, u) = F(z, u) \cdot \frac{F(z, u) - uF(uz, u)}{1 - u}
\]

(18)

for \( |u| < 1 \). Then, denoting by \( F^{(l)}(z, 1) \) the \( l \)th derivative of \( F(z, u) \) at \( u = 1 \), the \( r \)th factorial moment of \( d_n \) is

\[
\mathbb{E}[d_n(d_n - 1) \cdots (d_n - r + 1)] = \frac{\left[z^n\right]F^{(r)}(z, 1)}{\left[z^n\right]F^{(0)}(z, 1)}.
\]

We must solve (18) in order to compute the factorial moments. We shall follow now Knuth’s solution [40]. After introducing

\[
A_n(u) = (u - 1)^n F_n(u),
B_n(u) = (u^n - 1)A_{n-1}(u),
\]

we observe that the exponential generating functions \( A(z, u) \) and \( B(z, u) \) satisfy

\[
A(z, u) = e^{B(z, u)}.
\]

But \( C_n(u) = A_{n-1}(u) \) becomes

\[
B(z, u) = C(zu, u) - C(z, u),
\]

and

\[
C'_z(z, u) = A(z, u) = e^{C(zu, u) - C(z, u)}.
\]

Finally, the substitution \( G(z, u) = e^{C(z, u)} \) leads to

\[
G'_z(z, u) = G(zu, u)
\]

which translates into

\[
u^n G_n(u) = G_{n+1}(u).
\]

Therefore,

\[
G(z, u) = \sum_{n=0}^{\infty} u^{n(n-1)/2} \frac{z^n}{n!},
\]

and finally (with \( u = 1 + w \))

\[
\sum_{n=1}^{\infty} w^{n-1} F_{n-1}(1 + w) \frac{z^n}{n!} = \ln \left( \sum_{n=0}^{\infty} (1 + w)^{n(n-1)/2} \frac{z^n}{n!} \right).
\]

(19)

At this point Knuth observes that the right-hand side of (19) is the exponential generating function for labeled connected graphs. After introducing the exponential generating function

\[
W_k(z) = \sum_{n=1}^{\infty} C_{n-1+k, n} \frac{z^n}{n!}
\]

13
where \( C_{m,n} \) is the number of connected labeled graphs on \( n \) vertices and \( m \) edges, Knuth concludes that
\[
F(z, 1 + w) = W_0'(z) + w W_1'(z) + w^2 W_2'(z) + \cdots.
\]
But \( W_k(z) \) can be expressed in term of the tree-generating function \( T(z) \) defined in (1). Using Wright’s construction [67] (cf. also [31]) Knuth finally arrives at
\[
F(z, 1 + w) = \frac{T(z)}{z} f(w, T(z))
\]
where \( f(w, t) \) has the following leading terms
\[
f(w, t) = 1 + w \frac{t^2}{2(1 - t)^2} + O(w^2).
\]
This allows to compute all factorial moments of the total displacement. In particular,
\[
\text{Var}[d_n] = \frac{10 - 3\pi}{24} n^3 + \frac{16 - 3\pi}{144} n^2 + O(n^{3/2}),
\]
which solves the 35 year old problem of Knuth. As a matter of fact, an exact formula through the function \( Q_r(m, n) \) on the variance can be derived as shown in [23, 40]. Even more, Flajolet, Poblete and Viola were able to prove that \( \frac{d_n}{(n/2)^{3/2}} \) has the Airy distribution. I refer the interested reader to [23] for details of the derivations.

As a consequence of the results presented in [23, 40], combinatorial relationships between total displacement in linear probing, connectivity in graphs, inversions in trees, area of excursions and path length in trees, were re-discovered and placed in an unified framework. This initiated several new research lines in the AoF community, and will be further discussed in the forthcoming Part II of this article.

Finally, we devote the last part of this survey to “an exciting paper” by B. Vallée [64] who completed the work of Brent [4] on the analysis of the binary greatest common divisor (gcd) algorithm. Let us recall that the Euclidean gcd algorithm finds the greatest common divisor of two integers, say \( u \) and \( v \) by using divisions and exchanges as below:
\[
gcd(u, v) = \gcd(v \mod u, u).
\]
Heilbronn and Dixon proved independently that the average number \( D_N \) of divisions on random inputs less than \( N \) is asymptotically
\[
D_n \sim \frac{12 \log 2}{\pi^2} \log N.
\]

However, there is a more efficient implementation of the Euclidean algorithm called the binary gcd that does not require divisions. It works as follows: Let
\[
\text{val}_2(u) := \max\{b : 2^b | u\},
\]
that is, the largest \( b \) such that \( 2^b \) divides \( u \). The binary Euclidean algorithm is based on the following recursion
\[
gcd(u, v) = \gcd\left(\frac{u - v}{2^{\text{val}_2(u-v)}}, v\right).
\]
The challenge is to analyze the number of operations of this algorithm.

Vallée first reduces the problem to a continued fraction expansion. Indeed, observe that

\[ v = u + 2^{b_1}v_1, \quad v_1 = u + 2^{b_2}v_2, \quad v_{l-1} = u + 2^{b_l}v_l \]

represent the sequence of the shifts until the first interchange between \( u \) and \( v \) occurs. If \( k = b_1 + b_2 + \cdots + b_l \) and

\[ a = 1 + 2^{b_{1}} + \cdots + 2^{b_{1} + b_{2} + \cdots + b_{l-1}}, \]

then

\[ \frac{u}{v} = \frac{1}{a + 2^k \frac{u}{v}}. \]

In general, the rational \( u/v \) has a unique continued fraction expression:

\[ \frac{u}{v} = \frac{1}{a_1 + \frac{2^{k_1}}{a_2 + \frac{2^{k_2}}{a_3 + \cdots \frac{2^{k_{r-1}}}{a_r + 2^{k_r}}}}}. \]

The parameters of interest are:

- The height or the depth (it equals the number of exchanges); here, it is equal to \( r \).
- The total number of operations that are necessary to obtain the expansion: if \( p(a) \) denotes the number of 1 in the binary expansion of the integer \( a \), it is equal to \( p(a_1) + p(a_2) + \cdots + p(a_r) - 1 \), when the \( a_i \)'s are the denominators of the binary continued fraction.
- The total sum of exponents of 2 in the numerators of the binary continued fraction: here, it is equal to \( k_1 + k_2 + \cdots + k_r \).

Vallée analyzes these three parameters in a uniform manner using an operator called now the Vallée operator:

\[ V_2[f](x) := \sum_{k \geq 1} \sum_{a \text{ odd}, 1 \leq a < 2^k} \left( \frac{1}{a + 2^k x} \right)^2 f \left( \frac{1}{a + 2^k x} \right), \]

defined on a suitable Hardy space of holomorphic functions inside a disk that contains the real segment \([0, 1] \). Vallée proves that all three parameters are asymptotic to \( A \log N \) where the constant \( A \) depends on the dominant eigenvector of the operator \( V_2 \).

Briefly, Vallée uses various tools to prove her results such as generating functions, Ruelle operators, Tauberian methods, functional analysis. First, she applies classical tools of analysis of algorithms, namely generating functions which in the context of computational number theory are Dirichlet series. Second, Vallée shows that these generating functions are closely linked to the operator

\[ V_3[f](x) := \sum_{k \geq 1} \sum_{a \text{ odd}, 1 \leq a < 2^k} \left( \frac{1}{a + 2^k x} \right)^3 f \left( \frac{1}{a + 2^k x} \right). \]
which is a Ruelle operator. More precisely, the generating functions involve the quasi-inverse operator \( \Lambda_s := (I - V_s)^{-1} \), and the expectations of parameters of interest are partial sums of coefficients of these Dirichlet series. Thus the main results follow from an application of Tauberian Theorems due to Delange, provided that they can be applied. Vallée proves this is the case by showing that the operator \( V_s \) acting in a suitable Banach space has a “spectral gap”, i.e. a unique dominant eigenvalue separated from the remainder of the spectrum by a gap. When acting on a Hardy space of holomorphic functions relative to a suitable disk, the operator \( V_s \) is proven to be compact and positive for real values of parameter \( s \), and then it has a spectral gap. Since Tauberian theorems link the asymptotics of coefficients to the dominant singularity of the function, the constant \( A \) involves the dominant singularity of the quasi-inverse \((I - V_s)^{-1}\).

In summary, a consequence is that the binary gcd algorithm has average-case complexity asymptotic to \( A \log N \), where \( A \) is a computable constant that is mathematically well-characterized in terms of spectral characteristics of Vallée’s operator.

5 Conclusion

In this survey we briefly reviewed the first three meetings in Schloss Dagstuhl (so called “Dagstuhl Period”) of the newly created Analysis of Algorithms Group. We presented some ideas, solutions, and discussed some open problems. In Part II we shall describe the next five meetings of AofA that starting from 1998 became annual events.

The emergence of AofA as an organized field of research, which began with the Dagstuhl seminars, started a transformation from a collection of results on individual problems to a study of methods of general applicability, to an understanding of relationships to classical methods of analysis, combinatorics, and discrete probability, to a web of knowledge that applies in a broad context.

As D. E. Knuth mentioned in the conclusion of his paper [40], none of the methods he used in his work on linear probing hashing were available in 1962. We are now in a much better situation. Knuth himself popularized the field in his three volumes of The Art of Computer Programming [37, 38, 39], and quite recently in Selected Papers on Analysis of Algorithms [41]. Sedgewick and Flajolet prepared the first undergraduate textbook [59] that is widely used. They are in the process of writing a monograph on Analytic Combinatorics (cf. http://pauillac.inria.fr/algo/flajolet/Publications/books.html). H. Hamoud and M. Hofri contributed to popularizing the area by publishing fine books [25, 45, 46], while A. Odlyzko taught us in [50] the art of asymptotics. Finally, I myself put up a book on Average Case Analysis of Algorithms on Sequences [63] devoted to probabilistic and analytic methods used in analysis of algorithms. The reader is referred to these books as a good starting point to learn more about our field.

In passing we should finally add that in 1997 Philippe Flajolet and Helmut Prodinger started a webpage of AofA. Everybody is invited to http://pauillac.inria.fr/algo/AofA/ to read about fascinating story about linear probing hashing, binary Euclidean algorithms, wobbles in analysis of algorithms, and other new developments.
Acknowledgment

M. Drmota, P. Flajolet, H. Prodinger, B. Sedgewick, B. Vallée and A. Viola kindly provided comments to earlier drafts. I thank them whole-heartily.

References


