University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Doctor of Philosophy

of

# KHODAKHAST BIBAK

MMath (University of Waterloo, 2013)

## "Number Theoretic Methods and their Significance in Computer Science, Information Theory, Combinatorics, and Geometry"

Department of Computer Science

Thursday, April 6, 2017
1:00 P.M.
David Turpin Building
Room A137

Supervisory Committee:
Dr. Bruce M. Kapron, Department of Computer Science, University of Victoria (Co-Supervisor)
Dr. Venkatesh Srinivasan, Department of Computer Science, UVic (Co-Supervisor)
Dr. T. Aaron Gulliver, Department of Electrical and Computer Engineering, UVic (Outside Member)

External Examiner:
Dr. Michael J. Jacobson Jr., Department of Computer Science, University of Calgary

Chair of Oral Examination:
Dr. Michael McGuire, Department of Electrical and Computer Engineering, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

## Abstract

In this dissertation, I introduce some number theoretic methods and discuss their intriguing applications to a variety of problems in computer science, information theory, combinatorics, and geometry. First, using properties of Ramanujan sums and of the discrete Fourier transform of arithmetic functions, we give an explicit formula for the number of solutions of restricted linear congruences in their `most general case'. As a consequence, we derive necessary and sufficient conditions under which these congruences have no solutions. The number of solutions of this kind of congruence was first considered by Rademacher in 1925 and Brauer in 1926, in a special case. Since then, this problem has been studied, in several other special cases, in many papers. The problem is very well-motivated and has found intriguing applications in several areas of mathematics, computer science, and physics, and there is promise for more applications/implications in these or other directions.

Universal hash functions, discovered by Carter and Wegman in 1979, have many important applications in computer science. Applying our results we construct an almost-universal hash function family using which we give a generalization of a recent authentication code with secrecy scheme.

As another application of our results, we prove an explicit and practical formula for the number of surface-kernel epimorphisms from a co-compact Fuchsian group to a cyclic group. This problem has important applications in combinatorics, geometry, string theory, and quantum field theory (QFT). As a consequence, we obtain an `equivalent' form of Harvey's famous theorem on the cyclic groups of automorphisms of compact Riemann surfaces.

We also consider the number of solutions of linear congruences with distinct coordinates, and using a graph theoretic method, generalize a result of Schönemann from 1839. Also, we give explicit formulas for the number of solutions of unweighted linear congruences with distinct coordinates. Our main tools are properties of Ramanujan sums and of the discrete Fourier transform of arithmetic functions. Then,

as an application, we derive an explicit formula for the number of codewords in the Varshamov{Tenengolts code $VT_b(n)$ with Hamming weight k, that is, with exactly *k* 1's. The Varshamov{Tenengolts codes are an important class of codes that are capable of correcting asymmetric errors on a Z-channel. As another application, we derive Sloane's formula for the number of codewords in $VT_b(n)$, that is, $|VT_b(n)|$. We even go further and discuss applications to several other combinatorial problems, some of which have appeared in seemingly unrelated contexts. This provides a general framework and gives new insight into all of these problems which might lead to further work.

Finally, we bring a very deep result of Pierre Deligne into the area of coding theory | we connect Lee codes to Ramanujan graphs by showing that the Cayley graphs associated with some quasi-perfect Lee codes are Ramanujan graphs (this solves a recent conjecture). Our main tools are Deligne's bound from 1977 for estimating a particular kind of trigonometric sum and a result of Lovász from 1975 (or of Babai from 1979) which gives the eigenvalues of Cayley graphs of finite Abelian groups. Our proof techniques may motivate more work in the interactions between spectral graph theory, character theory, and coding theory, and may provide new ideas towards the long-standing Golomb-Welch conjecture.