Research Contributions Overview

Shmuel Onn

June 2010

My research concerns the development of efficient algebraic and geometric methods for discrete optimization, the investigation of the underlying mathematical structures, and the employment of such methods to applications in engineering and science. Below I describe some of my contributions, with emphasis on recent exciting developments in collaboration with several colleagues, which pave the way to an innovative comprehensive algorithmic theory of nonlinear discrete optimization, now culminating in my just-completed monograph **Nonlinear Discrete Optimization: An Algorithmic Theory** [1], based on my Nachdiplom Lectures given at ETH Zürich in Spring 2009.

Most recent parts of the research described below were done at Technion, ETH Zürich, University of California at Davis, MSRI (Mathematical Sciences Research Institute) Berkeley, and during two Research-in-Pair stays at MFO (Mathematisches Forschungsinstitut Oberwolfach), Germany.

Much of the research described below, recent and earlier, is the outcome of work with many colleagues. In particular, I have extensively collaborated (coauthored at least three joint papers) with Imre Bárány, Yael Berstein, Jesus De Loera, Antoine Deza, Raymond Hemmecke, Frank Hwang, Peter Kleinschmidt, Jon Lee, Uriel Rothblum, Bernd Sturmfels, and Robert Weismantel.

Nonlinear Integer Programming and Applications.

Integer programming is a fundamental framework for discrete optimization problems where the feasible solutions are the integer points satisfying a system of linear inequalities. It has very broad modeling power, but, unless the dimension is fixed, is generally computationally intractable.

Yet, in a recent series of pioneering papers [3, 4, 5, 6], combining recent algebraic and geometric methods, we were able to show that Graver bases enable to solve linear and nonlinear integer programming problems in variable dimension in polynomial time. A comprehensive treatment of some of this theory can be found in my recent broad article [2]. Our results include the following:

- Linear integer programming [3], convex maximization [4], and convex minimization [5];
- Non-convex optimization of broad classes of quadratic and higher degree polynomials [6].

In particular, these results lead to genuine polynomial time algorithms for integer programming in variable dimension over multi-way tables and more generally over n-fold systems. These are broad fundamental classes which basically include any problem with multiply indexed variables, in particular various packing problems, partitioning problems, multi-commodity flow problems, and more. In fact, *every* integer program *is* a suitable n-fold program, making such problems universal in a well defined sense [16, 17]; this universality is discussed in more detail in the sequel. Among other results, we establish polynomial time algorithms for the following problems in variable dimension:

- Convex maximization [4] and minimization [5] over n-fold systems and multi-way tables;
- Linear optimization and convex maximization over stochastic integer programs [5].

Some of the many applications of this algorithmic theory are the following:

- *Privacy and disclosure control in statistical databases*: in [18, 19], see more details below;
- *Multi-commodity transshipment, multi-way transportation, and multi-commodity b-matching*: with linear or nonlinear, congestion-dependent, objective functions [7, 8];
- *Error-correcting codes*: we can recover a message transmitted over a noisy channel as the one that satisfies pre-agreed check sums and is l_p-closest to the received distorted message [5];
- *Machine scheduling, bin packing and cutting stock*: we provide new algorithms for such problems and our results seem to shed new light on some fundamental intriguing problems concerning integer rounding and the complexity for fixed number of job lengths [3, 4];

Our work also suggests a practical *Graver based approximation scheme*, currently under study, which uses increasingly better approximations of the underlying Graver bases and may quickly provide approximative solutions for large scale nonlinear integer programming over multi-way tables, n-fold systems, stochastic n-scenario systems, and possibly integer programming more generally.

Invited presentations of this work include the Nachdiplom Lectures at ETH Zürich (Spring 2009), and Main Speaker talks at IPAM (Institute for Pure and Applied Mathematics) Workshop on Discrete Optimization, UCLA (coming October 2010), Lecture Series at MSRI (Mathematical Sciences Research Institute) Summer Graduate Workshop, Berkeley (coming August 2010), CREST–SBM International Conference on Harmony of Gröbner Bases and the Modern Industrial Society, Osaka, Japan (coming June 2010), MIP 2009 – Mixed Integer Programming Workshop Series, UC - Berkeley (June 2009), IMA (Institute for Mathematics and its Applications) Hot Topics Workshop: Mixed-Integer Nonlinear Optimization: Algorithmic Advances and Applications, University of Minnesota (November 2008), and Billerafest, Cornell University, Ithaca (June 2008).

Nonlinear Combinatorial Optimization and Applications.

Combinatorial optimization problems form a fundamental class of discrete optimization problems where the set of feasible solutions is a family of subsets of a finite universe and is presented implicitly, often by one of various types of oracles. Since such problems are often computationally intractable, much of the extensive literature on the subject has concentrated on linear objectives functions, that often provide only an approximation of the real underlying applications they aim to model.

But, in our paper [10] (awarded the ORSIS Prize for Best Research Paper), we were able to identify a geometric condition on a family of subsets - being *edge-well-behaved* - that enables to efficiently maximize convex objective functions over the family. More recently, in a series of papers [11, 12, 13, 14], we extended this to many combinatorial families and nonlinear objective functions, often of the natural form $f(x) = g(w_1 x, \ldots, w_d x)$, where the $w_i x$ represent various linear criteria and g provides a "balancing" compromising these multi-criteria. Our work advances an emerging comprehensive algorithmic theory of nonlinear combinatorial optimization, that enables:

- Maximization of convex objectives over any edge-well-behaved family presented by a membership oracle including matroids, partitioning and clustering, in strongly poly-time [9, 10];
- Optimization of nonlinear balanced multi-criteria objectives over matroids, in poly-time [11];
- Exact maximization and approximative minimization of broad classes of convex objective functions over any family presented by a linear optimization oracle, in polynomial time [12, 13];
- Randomized optimization of nonlinear balanced multi-criteria objectives over assignments, matchings in arbitrary graphs, and matroid intersections, in polynomial time [12, 13];
- In exciting recent work [14] we introduce a new kind of approximation and are able to compute an r-best solution for optimizing any nonlinear univariate function over any weighted independence system, with no special structure, presented by a linear optimization oracle, using properties of integer monoids and their Frobenius numbers, in polynomial time. In contrast, we show that finding an exact optimal solution requires *exponential time* [14, 15],

Some of the many applications of this algorithmic theory, discussed in [9, 10, 11, 12, 13, 14] are:

- *Experimental design and learning*: in this important ongoing multidisciplinary project with statisticians [11] we wish to learn an unknown system using experiments or queries, by feeding the system with various inputs and measuring its outputs. Using our results on nonlinear matroid optimization, we can learn the system and fit a sparse multivariate polynomial model of smallest *abberation*. Many issues in classical experimental design theory, such as the *inverse problem* of choosing an optimal design, become algorithmically accessible by our methods.
- *Partitioning and Clustering*: we can partition multi-criteria evaluated items to players so as to maximize social utility that is a convex function of the sums of multi-criteria values of items each player gets, and find a minimum variance clustering of a set of points in space [10];
- *Multi-criteria network connectivity*: in a network where each edge has a vector of weights representing its multi-criteria evaluation, we can find a spanning subnetwork that optimizes an arbitrary nonlinear function of the sum of multi-criteria vectors of its edges [9, 10, 11];
- *Assignment, Scheduling and Exact Matching*: we can find (in a randomized way) assignments optimizing nonlinear objectives, we can approximate a minimum make-span scheduling, and our work seems to shed new light on the long open notorious exact matching problem [12];
- *Gröbner Bases*: the methods of [9, 10] are implicitly used in computing universal Gröbner bases of systems of polynomials in [24] (see more detailed discussion on Gröbner bases below).

Invited presentations of this work include keynote lecture on winning the ORSIS Prize, Caesarea (May 2005), Lecture Series, SMS-Montréal (June 2006), ZIB - Berlin (July 2005), Cube Workshop, Magdeburg (July 2005), and Mathematical Sciences Research Institute, Berkeley (September 2003).

Universality of Multi-Way Transportation Problems and Privacy in Data Bases.

High dimensional transportation problems concern optimization over multi-way tables and form a very important and useful class of discrete optimization problems. In a recent series of papers [16, 17, 18] we made several striking discoveries about such problems. In particular, we have shown that "short", $r \times c \times 3$, transportation problems are *universal* in the very strong sense that every linear and integer program can be efficiently lifted to some $r \times c \times 3$ transportation problem while transforming the real and integer points bijectively. This universality theorem resolved several standing open problems and has important consequences for linear and integer programming.

In contrast, our work [3, 4, 5] on nonlinear integer programming over n-fold systems (discussed before) implies that "long" transportation problems, over $m_1 \times \cdots \times m_{d-1} \times n$ tables of any dimension d with one long variable side n, can be treated in polynomial time. In particular, nonlinear congestion-dependent objectives can be minimized over such integer long tables in polynomial time.

Privacy in data bases. An extremely important application area concerns web-disclosure of sensitive data by public agencies such as the Census Bureau or National Institute for Health Statistics. It is a common practice in the disclosure of multi-way tables containing sensitive data to release some of the table margins rather than the table itself. This framework raises many algorithmic problems regarding the set of possible tables having the same margins as the released ones. For instance, a fundamental problem is whether a certain table entry is uniquely determined by the disclosed margins: if it is, then that entry is vulnerable; otherwise it may be assumed secure.

Our work on n-fold systems leads to an efficient solution of this entry uniqueness problem [19]. This may allow agencies to efficiently check vulnerability of sensitive entries and make learned decisions about secure disclosure, refraining from disclosure or releasing fewer margins when necessary.

This work was presented in the Eurostat Conference on Privacy in Statistical Databases held in the Italian National Institute of Statistics in Rome during December 2006 and was perceived with great excitement. In discussions with colleagues involved in data disclosure policy making at the U.S. Census Bureau and National Institute for Health Statistics on several occasions, many other more issues arise, concerning the structure of entry values, the collapsing of some table factors to make vulnerable entries become secure, choice of margins sufficiently informative for data users but not exposing sensitive entries, and modification of entries by adding noise to make disclosure safe without too much distortion. Our efficient algorithms for nonlinear optimization over multi-way tables and the ability to find a table which is l_p-closest to a destination table in [3, 4, 5] promise computationally efficient access to such problems, but much more investigation is to be done.

Invited presentations of this work include talks as Main Speaker at the Mathematical Research Institute at ETH, Zurich (May 2006) and at the Conference on Theoretical and Practical Effectivity of Gröbner Bases in Tokyo (August 2005), and talks at the Privacy Day at the Weizmann Institute (July 2006), the International Research Station, Banff, Canada (March 2006), the Mathematical Research Institute Oberwolfach (August 2004), and the American Institute of Mathematics, Palo Alto (December 2003). It was also presented at IPCO 10, Columbia University (June 2004).

Convex Partitioning Problems.

The class of partitioning problems is a very rich class of discrete optimization problems which naturally captures a wide range of operations research applications such as load balancing, ranking, cluster analysis, and more. In a series of papers including [20, 21, 22, 23], we introduce a unified approach, based on vectorial partitions, for such problems. Using geometric methods, we provide:

- A hierarchy of polynomial time algorithms for partition problems with convex objective functions, parameterized by the number of criteria and parts, which leads to efficient algorithms for many new problems and subsumes existing ad-hoc algorithms for others [21, 22, 23];
- The asymptotical behavior of the maximum number of separable partitions in Euclidean space and spaces of finite Vapnik-Chervonenkis dimension [20] (*Editors' Choice* selected paper).

Invited presentations of this work include a double-lecture at the Berlin-Zürich Colloquium Series at ETH (April 2001) and the Mathematical Research Institute Oberwolfach (February 1999).

Gröbner Bases Theory and Applications.

Systems of multi-variate polynomial equations are useful in a variety of applications areas. In particular, the set of feasible solutions of any discrete optimization problem can be quite easily encoded as the set of roots of a system of polynomials. Gröbner bases provide the engine for computations with such systems of polynomials. In our work in this area we have been able to:

- Devise polynomial time algorithms for computing all Gröbner bases and the universal Gröbner basis of any system of polynomials with finite set of roots in fixed number of variables [24] using geometric ideas, in contrast with the general doubly exponential time complexity;
- For generic systems, construct the universal Gröbner basis and explicitly coordinatize the vertices of the *state polytope* that index the distinct Gröbner bases of the system [25];
- Employ Gröbner bases methods for automated transformation of systems of partial differential equations to formulations that are more accessible to numerical solution, providing a powerful set of tools for handling large systems of partial differential equations [26];
- Characterize and decompose Gröbner bases of modules associated with group-representations, thereby enabling the computation of numerical invariants and other information about the group-representation by Gröbner bases methods [27].

Invited presentations of this work include talk as Main Speaker at the Conference on Theoretical and Practical Effectivity of Gröbner Bases in Tokyo (August 2005) and talks at the Mathematical Research Institute Oberwolfach (June 2002) and Operations Research Center at MIT (April 2002).

Some Other Contributions.

- *Ellipsoid and other Optimality Certificates.* In [28] we show that the ellipsoid method can be efficiently augmented with the computation of proximity certificates for a variety of continuous problems with convex structure including convex minimization, variational inequalities with monotone operators, and computation of Nash equilibria in convex games. In [29] we introduce several optimality test sets for integer optimization with nonlinear objective functions.

- *Nullstellensatz Certificates and Combinatorial Optimization.* As mentioned when discussing Gröbner bases, combinatorial optimization problems can be encoded in systems of polynomial equations. Hilbert's Nullstellensatz can then provide infeasibility certificates. In [30] we develop this for nowhere-zero flows and in [31] for stable sets, colorability, and Hamiltonicity.

- *Colourful Linear Programming.* In [32, 33] we introduce and study *colourful linear programming*, whose expressive power and complexity interpolates between linear programming and integer programming. We provide efficient approximation algorithms for the problem and discuss several relatives including Tverberg partitions and integer Radon partitions [34].

- *Artificial-Intelligence Multi-Agent Routing.* In a variety of applications, agents such as robots or messages are required to be routed without collisions on a network, with destinations changing dynamically and individually. While centralized routing is intractable, in [35, 36] we provide a procedure for synthesizing navigation rules on the network, that once obeyed by all agents, allow each agent to devise a motion plan that will take it to any desired destination without collisions and regardless of its present location and the behavior of the other agents.

- *Counting and a Theory of Signable Posets and Oriented Matroids.* In [37, 38, 39] we introduce and develop a theory of *signable partially ordered sets* that extends and unifies the theories of shellable posets and partitionable simplicial complexes. We show that broad classes of spheres including polyhedral fans and oriented matroid polytopes are signable. While counting faces is typically intractable, our theory leads to polynomial time counting in certain situations.

- *Pivoting and Diameter of Polytopes.* Motivated by the behavior of pivoting algorithms for linear programming and the long open polynomial Hirsch problem on the diameter of polytopes, we establish in [40] polynomial bounds on the diameter of lattice-sparse polytopes, and in [41], bounds on the diameter of multi-index polytopes (shown to be universal in [17]).

- *Grid Representation of Polytopes.* Small grid embedding of polyhedral objects is advantageous for their computerized manipulation. In [42] we established the first singly exponential upper bound on the grid size sufficient to host any 3-polytope in terms of the number of vertices. Whether a polynomial bound can be attained remains a challenging and long open problem.

- *Combinatorial Optimization and Permutation Polytopes.* Representations of the symmetric group provide a natural framework that allows a unified treatment of combinatorial optimization problems by encoding them as problems of linear optimization over suitable orbits under the group action. In [44] we investigate this framework and the stratification of space by the orbit polytope type. Understanding the deformation of sequences of orbits of low computational complexity to orbits of high complexity remains an important issue for investigation. In [43] we further investigate this in connection with the graph isomorphism problem.

Invited presentations of some of this (mostly earlier) work include at the University of California, Berkeley (February 1996), workshops on Convex Polytopes and Algebraic Combinatorics, Jerusalem (December 1996 and May 1993), Università di Padova, Padova (February 1995), workshop on Combinatorial and Computational Geometry, Eilat (March 1995), Mathematical Research Institute Oberwolfach (February 1995 and January 1992), ZIB, Berlin (November 1993), Charles University, Prague (October 1993), Princeton University (May 1993), American Mathematical Society Annual Meeting, San Antonio (January 1993), Courant Institute, New York University (December 1992), Institut Mittag-Leffler, Stockholm (May 1992), University of California at San Diego (November 1991), and at the MSI workshop on Discrete and Combinatorial Geometry, Ithaca (July 1991).

References

[1] S. Onn, Monograph, **Nonlinear Discrete Optimization: An Algorithmic Theory**, *Zurich Lectures in Advanced Mathematics*, European Mathematical Society, 1–150, to appear

(The monrgraph is based on my Nachdiplom Lectures given at ETH Zürich in Spring 2009. Partial lecture notes are available at `http://ie.technion.ac.il/~onn/Nachdiplom/`.)

[2] S. Onn, Theory and Applications of N-Fold Integer Programming, IMA Volume on Mixed Integer Nonlinear Programming, Frontier Series, Springer, pages 1–35, to appear

[3] N-fold integer programming (with J. De Loera, R. Hemmecke, R. Weismantel), *Discrete Optimization*, 5:231–241 (2008)

[4] Convex Integer Maximization via Graver Bases (with J. De Loera, R. Hemmecke, U.G. Rothblum, R. Weismantel), *Journal of Pure and Applied Algebra*, 213:1569–1577 (2009)

[5] A polynomial oracle-time algorithm for convex integer minimization (with R. Hemmecke, R. Weismantel), *Mathematical Programming*, pages 1–21, to appear

[6] The quadratic Graver cone, quadratic integer minimization, and extensions (with J. Lee, L. Romanchuk, R. Weismantel), submitted

[7] The Graver complexity of integer programming (with Y. Berstein), *Annals of Combinatorics*, 13:289–296 (2009)

[8] N-fold integer programming and nonlinear multi-transshipment (with R. Hemmecke, R. Weismantel), submitted.

[9] Convex matroid optimization, *SIAM Journal on Discrete Mathematics* 17:249–253 (2003)

[10] Convex combinatorial optimization (with U.G. Rothblum), *Discrete and Computational Geometry* 32:549–566 (2004), **Winner of the Operations Research Society of Israel (ORSIS) 2005 Prize for Best Research Paper in Operations Research.**

[11] Nonlinear matroid optimization and experimental design (with Y. Berstein, J. Lee, H. Maruri-Aguilar, E. Riccomagno, R. Weismantel, H. Wynn), *SIAM Journal on Discrete Mathematics*, 22:901–919 (2008)

[12] Nonlinear bipartite matching (with Y. Berstein), *Discrete Optimization*, 5:53–65 (2008), **Winner of the Operations Research Society of Israel (ORSIS) 2008 Abraham Mechrez Prize for Best Student Paper.**

[13] Parametric nonlinear discrete optimization over well-described sets and matroid intersections, (with Y. Berstein, J. Lee, R. Weismantel), manuscript in preparation *Mathematical Programming*, pages 1–21, to appear

[14] Approximate nonlinear optimization over weighted independence systems (with J. Lee, R. Weismantel), *SIAM Journal on Discrete Mathematics*, 23:1667–1681 (2009)

[15] Intractability of approximate multi-dimensional nonlinear optimization on independence systems (with J. Lee, R. Weismantel), submitted

[16] The complexity of three-way statistical tables (with J. De Loera), *SIAM Journal on Computing* 33:819–836 (2004)

[17] All linear and integer programs are slim 3-way transportation programs (with J. De Loera), *SIAM Journal on Optimization* 17:806–821 (2006)

[18] Markov bases of three-way tables are arbitrarily complicated (with J. De Loera), *Journal of Symbolic Computation* 41:173–181 (2006)

[19] Entry Uniqueness in Margined Tables, in: Privacy in Statistical Databases, PSD 2006 Proceedings (J. Domingo-Ferrer and L. Franconi eds.), Lecture Notes in Computer Science 4302:94–101 (2006)

[20] Separable partitions (with N. Alon), *Discrete Applied Mathematics* 91:39–51 (1999), **Selected for Discrete Applied Mathematics Editors' Choice**, `http://www.elsevier.com/homepage/sac/disc/edchoice/dam1999.html`

[21] A polynomial time algorithm for shaped partition problems (with F.K. Hwang, U.G. Rothblum), *SIAM Journal on Optimization* 10:70–81 (1999)

[22] Linear shaped partition problems (with F.K. Hwang, U.G. Rothblum), *Operations Research Letters* 26:159–163 (2000)

[23] The vector partition problem for convex objective functions (with L.J. Schulman), *Mathematics of Operations Research* 26:583–590 (2001)

[24] The Hilbert zonotope and a polynomial time algorithm for universal Gröbner bases (with E. Babson, R. Thomas), *Advances in Applied Mathematics* 30:529–544 (2003)

[25] Cutting Corners (with B. Sturmfels), *Advances in Applied Mathematics* 23:29–48 (1999)

[26] Automated transformations for PDE systems with applications to multigrid solvers (with Y. Gil, Z. Gutterman, I. Yavneh), *SIAM Journal on Scientific Computing* 24:886–904 (2002)

[27] Hilbert series of group representations and Gröbner bases for generic modules, *Journal of Algebraic Combinatorics* 3:187–206 (1994)

[28] Accuracy certificates for computational problems with convex structure (with A. Nemirovski, U.G. Rothblum), *Mathematics of Operations Research*, 35:52–78 (2010)

[29] On test sets for nonlinear integer maximization (with J. Lee, R. Weismantel), *Operations Research Letters*, 36:439–443 (2008)

[30] Nowhere-zero flow polynomials, *Journal of Combinatorial Theory Series A*, 108:205–215 (2004)

[31] Expressing combinatorial optimization problems by systems of polynomial equations and the Nullstellensatz (with J. De Loera, J. Lee, S. Margulies), *Combinatorics, Probability and Computing*, 18:551–582 (2009)

[32] Colourful linear programming (with I. Bárány), in: Integer Programming and Combinatorial Optimization, 5th IPCO Proceedings (W.H. Cunningham, S.T. McCormick and M. Queyranne eds.), Lecture Notes in Computer Science 1084:1–15 (1996)

[33] Colourful linear programming and its relatives (with I. Bárány), *Mathematics of Operations Research* 22:550–567 (1997)

[34] On the geometry and computational complexity of Radon partitions in the integer lattice, *SIAM Journal on Discrete Mathematics* 4:436–447 (1991)

[35] Determination of social laws for multi-agent mobilization (with M. Tennenholtz), *Artificial Intelligence* 95:155–167 (1997)

[36] Social network coordination and graph routing (with E. Sperber), *Networks* 41:44–50 (2003)

[37] Oriented matroid polytopes and polyhedral cone fans are signable (with P. Kleinschmidt), in: Integer Programming and Combinatorial Optimization, 4th IPCO Proceedings (E. Balas and J. Clausen eds.), Lecture Notes in Computer Science 920:198–211 (1995)

[38] Signable posets and partitionable simplicial complexes (with P. Kleinschmidt), *Discrete and Computational Geometry* 15:443–466 (1996)

[39] Strongly signable and partitionable posets, *European Journal of Combinatorics* 18:921–938 (1997)

[40] Lattice-free polytopes and their diameter (with M. Deza), *Discrete and Computational Geometry* 13:59–75 (1995)

[41] Graphs of transportation polytopes (with J. De Loera, E.D. Kim, F. Santos), *Journal of Combinatorial Theory Series A*, 116:1306-1325 (2009)

[42] A quantitative Steinitz' theorem (with B. Sturmfels), *Beiträge zur Algebra und Geometrie* 35:125–129 (1994)

[43] Two graph isomorphism polytopes, *Discrete Mathematics*, 309:2934–2936 (2009)

[44] Geometry, complexity, and combinatorics of permutation polytopes, *Journal of Combinatorial Theory Series A* 64:31–49 (1993)