The Specker-Blatter Theorem

In memory of Ernst P. Specker at the occasion of his centenary

J.A. Makowsky

Based on a survey paper by E. Fischer, T. Kotek and J.A. Makowsky "Application of logic to combinatorial sequences and their recurrence relations." Model Theoretic Methods in Finite Combinatorics 558 (2011): 1-42.

Abstract:

The Specker-Blatter Theorem states that number of labeled graphs over n vertices satisfying an MSOL-definable property satisfies a linear modular recurrence relation for every modulus m.

We give a gentle survey of the statement, the proof and applications.



Ernst Specker



Christian Blatter

- C.B and E.S: Le nombre de structures finies dune theoriea charactere fin, Sciences Mathématiques, Fonds Nationale de la recherche Scientifique, Bruxelles, 1981
- C.B and E.S: Modular periodicity of combinatorial sequences, Abstract Amer. Math. Soc, 1983
- C.B. and E.S.: Recurrence relations for the number of labeled structures on a finite set. In Logic and Machines: Decision Problems and Complexity (pp. 43-61). Springer Berlin/Heidelberg, 1984.
- **E.S.:** Application of logic and combinatorics to enumeration problems Trends in Theoretical Computer Science (E. Börger, ed.), 1988

scholar.google.com

 Ernst Speckers most cited paper, according to google scholar is:

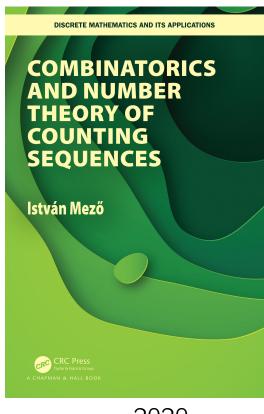
Kochen, Simon and Specker, Ernst P., The problem of hidden variables in quantum mechanics, reprinted in: The logico-algebraic approach to quantum mechanics, 293–328, 1975 Springer

with 3163 citations

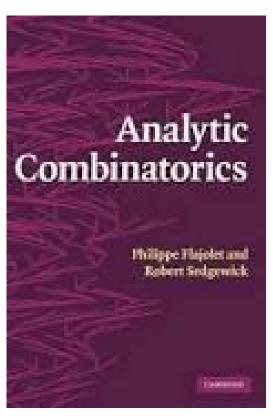
The talks after mine are about E. Specker's work in Quantum Mechanics

• I am going to talk about the least cited paper.

Before I started working on it, all its version had together had less than 10 citations.



2020



2009

Even these books do not mention this work

Congruences for combinatorial functions 1980



Ira Gessel



Philippe Flajolet

- Gessel, Ira.
 Congruences for Bell and tangent numbers.
 IBM Thomas J. Watson Research Division, 1978.
- Flajolet, Philippe. "On congruences and continued fractions for some classical combinatorial quantities."

 Discrete Mathematics 41.2 (1982): 145-153.

Congruences for combinatorial functions, one by one

In Mező's book we find only special cases......

- Bell and Tangent numbers
- Stirling numbers and harmonic numbers
- Fubini numbers

..... and no general theory.

Congruences for infinitely many

combinatorial functions

• Let P be a graph property, and let

$$d_P(n) = |\{E \subseteq [n]^2 : ([n], E) \in P\}|$$

be the number of ways one can find an edge relation E on the set $\{1,\ldots,n\}$ to obtain a graph $G=([n],E)\in P$.

- $d_P(n)$ is called the density function of P.
- If P is monotone (hereditary) it is called the speed of P.

C. Blatter and E. Specker study algebraic properties of density functions already in **1980**.

Only in 1994, E. Scheinerman and J. Zito initiate the study growth rates of density functions for hereditary properties, and relate thenm to structural properties of graphs $G \in P$.

How it all started?

Counting finite topologies

E. Specker teaches Introduction to Topology and gives homework. Let T_n be the number of topologies on the set $\{1, \ldots, n\}$.

 $T_1 = 1$, as the underlying set is always open.

 $T_2 = 4$, for each singleton, we can decide whether it is open or not.

 T_n is bounded by 2^{2^n} , hence $T_5 \leq 2^{32}$.

Two papers, and a disturbing fact

 $T_5 = 7181$

A. Shaafat, On the number of topologies definable for a finite,

J. Australian Mat. Soc., vol 8 (1968), 194-198.

$$T_5 = 6942$$

J. Evans, F. Harary and M.S. Lynn, *On the computer enumeration of finite toplogies*, Communications of the ACM, 10 (1967), 295-297.

The analysis by C. Blatter and E. Specker shows:

$$7181 \neq 2 \mod 5$$

$$6942 = 2 \mod 5$$

This allows us them conclude that

$$T_5 = 7181$$
 is not possible.

Logic and Combinatorics

- The class of finite topologies is not definable in First Order or even Second Order Logic.
- But the number of topologies on n points is the same as the number of reflexive transitive relations on n points.
- The class of reflexive transitive relations on n points is definable in First Order Logic.

E. Specker thought that counting First Order definable relations should be amenable using techniques from logic.

The original theorem

(C. Blatter and E. Specker 1980)

Let P be a property of structures $(A, R_i), i \in [k]$, where

- (i) each R_i is a unary or binary relation,
- (ii) P is definable using Monadic Second Order Logic MSOL,

Let d_P the density function for P and d_P^m be the sequence

$$d_P^m(i) = d_P(i) \mod m$$
.

Then $d_P^m(i): i \in \mathbb{N}$ is ultimately periodic.

It was left open, whether

- (i) the restriction in (i) to at most binary relations was necessary, and
- (ii) the restriction in (ii) to MSOL among fragments of Second Order Logic SOL was necessary.

The density function for regular graphs

J.H. Redfield's Theorem, 1927

The class REG_r of simple regular graphs where every vertex has degree r is FOL-definable (for fixed r).

Counting the number of labeled regular graphs is treated completely in Chapter 7 of the book:

Harary, Frank, and Edgar M. Palmer. Graphical enumeration, 1973, reprinted by Elsevier, 2014.

where an explicit formula is given, essentially due to J.H. Redfield (1927) and rediscovered by R.C. Read (1959).

However, the formula is very complicated.

For cubic graphs, the function is explicitly given: $f_{\mathcal{R}_3}(2n+1)=0$ and

$$f_{\mathcal{R}_3}(2n) = \frac{(2n)!}{6^n} \sum_{j,k} \frac{(-1)^j (6k-2j)! 6^j}{(3k-j)! (2k-j)! (n-k)!} 48^k \sum_i \frac{(-1)^i j!}{(j-2i)! i!}$$

Can you see that this is ultimately periodic mod 17?

Regular graphs of even degree

- Eulerian graphs are connected regular graphs of even degree.
- Regular graphs of even degree are red not MSOL-definable, neither are Eulerian graphs.

Let CMSOL be the logic obtained from MSOL by adding modular counting quantifiers:

$$C_{m,a}(x)\phi(x)$$

which say that the set elements satsifying $\phi(x)$ in a finite structure $\mathfrak A$ has size a modulo m.

Regular graphs of even degree, and Eulerian graphs are CMSOL-definable.

What can we say about $d_{EULER}(n)$?

 $d_{EULER}(n)$ is not a special case of the Blatter-Specker Theorem!

Two equal-sized cliques

Let EQ_2 the class of finite graphs which consist of the disjoint unions of two equal-sized cliques.

 EQ_2 is not CMSOL-definable, but it is SOL-definable.

We look at its density function $d_{EQ_2}(n)$. We have

$$d_{EQ_2}(n) = \begin{cases} \frac{1}{2} {2m \choose m} & \text{for } n = 2m \\ 0 & \text{else} \end{cases}$$

The factor $\frac{1}{2}$ is there because we cannot distinguish the choice of the first clique from the choice of its complement.

Proposition: (Lucas, 1878)

For every n which is not a power of 2, we have $d_{EQ_2}(n) \equiv 0 \pmod{2}$, and for every n which is a power of 2 we have $d_{EQ_2}(n) \equiv 1 \pmod{2}$.

In particular, $d_{EQ_2}(n)$ is not ultimately periodic modulo 2.

A proof may be found as Exercise 5.61 in: R. Graham, D. Knuth and O. Patashnik, Concrete Mathematics, 2nd ed., Addison-Wesley 1994

A late birthday gift for E. Specker's 80th birthday

- I planned to write a paper attacking the then open problems related to the Blatter-Specker Theorem for E. Specker's 80th birtday.
- I spoke with him about it, and he was very skeptical;=).
- Indeed, I was late!
- From 2000 I started to lecture about this theorem.
- In 2002 Eldar Fischer, attending my lecture, found a counter example:

Theorem: There is a property of finite structures with one quaternary relation, which is evem **FOL**-definable but violates the Blatter Specker Theorem.

Fischer, Eldar. "The SpeckerBlatter theorem does not hold for quaternary relations." Journal of Combinatorial Theory, Series A 103.1 (2003): 121-136.

More recent work

E. Specker was intrigued and excited by Fischer's example.

Specker, E.
 "Modular Counting and Substitution of Structures."
 Combinatorics, Probability & Computing 14.1-2 (2005): 203.

E. Fischer, and later my PhD student T. Kotek and I analyzed the proof of the Blatter-Specker Theorem:

- Fischer, Eldar, and Johann A. Makowsky. "The Specker-Blatter theorem revisited." International Computing and Combinatorics Conference. Springer, Berlin, Heidelberg, 2003.
- Kotek, Tomer, and Johann A. Makowsky. "Definability of combinatorial functions and their linear recurrence relations." Fields of logic and computation. Springer, Berlin, Heidelberg, 2010. 444-462.

My collaborators



Eldar Fischer



Tomer Kotek

Fischer, Eldar, Tomer Kotek, and Johann A. Makowsky.
 "Application of logic to combinatorial sequences and their recurrence relations.",

in: Model Theoretic Methods in Finite Combinatorics, volume 558 of Contemporary Mathematics, (2011): 1-42.

Separating Logic from Combinatorics

C. Blatter and E. Specker associate with a property P of relational structures a rank, the substitution rank, with values in $\mathbb{N} \cup \{\infty\}$.

The logic part of their theorem is the following:

Proposition: If P is MSOL-definable this rank is finite.

We (EF and JAM) prove:

Proposition: If P is CMSOL-definable this rank is finite.

The rest of their (CB and ES) proof is algebra-combinatorial.

Proposition: If P is a property of structures with all relations at most binay, and P has finite rank, then $d_P^m(n)$ is ultimately periodic for every $m \in \mathbb{N}$.

This now covers also the case of **Eulerian graphs** and **regular graphs of even degree**.

Refining the analysis of the CB-ES proof

We also take into account the

maximal degree of the structures in P.

We generalize the Substitution rank of a property P using

Hankel matrices.

Relations of bounded degree

Let $\mathcal{A}=\langle A, \bar{R} \rangle$ be a τ -structure. We define a symmetric relation E_A on \mathcal{A} , and call $\langle A, E_A \rangle$ the Gaifman-graph of \mathcal{A} .

- Let $a, b \in A$. $(a, b) \in E_A$ iff there exists a relation $R \in \overline{R}$ and some $\overline{a} \in R$ such that both a and b appear in \overline{a} (possibly with other members of A as well).
- For any element $a \in A$, the degree of a is the number of elements $b \neq a$ for which $(a, b) \in E_A$.
- We say that A is of bounded degree d if every $a \in A$ has degree at most d.
- We say that A is connected if its Gaifman-graph is connected.
- For a class of structures \mathcal{P} we say it is of bounded degree d (resp. connected) iff all its structures are of bounded degree d (resp. connected).

File:sp-degree 20

The Specker-Blatter Theorem revisited, I

Theorem(E. Fischer and JAM, 2002)

Let \mathcal{P} be a property of τ -structures, which is CMSOL-definable. Let $d_{\mathcal{P}}(n)$ be its density function.

- If \mathcal{P} is of bounded degree d, the function $d_{\mathcal{P}}(n)$ satisfies a modular recurrence relation for every m.
- Furthermore, if additionally all the models in \mathcal{P} are connected, the function $f_{\mathcal{P}}$ satisfies the trivial recurrence relations for every m.

We have no restrictions on τ besides not allowing function symbols,

File:sp-degree 21

Hankel matrices for graph properties, I

- A k-graph of order n is a graph $G = (V(G), E(G), a_1, \ldots, a_k)$ with V(G) = [n] together with k distinct vertices a_1, \ldots, a_k .
- Let \square be a binary operation on k-graphs.
 - □ could be
 - (i) □, the disjoint union of graphs (without labels),
 - (ii) \sqcup_k , the k union of k-graphs formed by taking the disjoint union and then identifying corresponding distinct vertices.
 - (iii) or the substition S(G, H) of a 1-graph G for the distinct label a of the 1-graph H.

Hankel matrices for graph properties, II

- Let $G_i, i \in \mathbb{N}$ be an enumeration of all finite k-graphs.
- Let P be a graph property.
- We define the infinite (0,1)-matrix $\mathfrak{H}(P,\square)$ with

$$\mathfrak{H}(P,\square)_{i,j} = \begin{cases} 1 & G_i \square G_j \in P \\ 0 & G_i \square G_j \notin P \end{cases}$$

• We denote by $rk(P, \square)$ the rank of $\mathfrak{H}(P, \square)$ over the field \mathbb{Z}^2 .

The matrix $\mathfrak{H}(P,\square)$ is called the **Hankel matrix** of P and \square for k-graphs.

Unknowingly, C. Blatter and E. Specker use

a special case of Hankel matrices.

Hankel matrices (over a field \mathcal{F})

Let $f: \mathcal{F} \to \mathcal{F}$ be a function over a field \mathcal{F} .

A finite or infinite matrix $H(f) = h_{i,j}$ is a Hankel matrix for f if $H_{i,j} = f(i+j)$.

Hankel matrices have many applications in: numeric analysis, probability theory and combinatorics.

- Padé approximations
- Orthogonal polynomials
- Probability theory (theory of moments)
- Coding theory (BCH codes, Berlekamp-Massey algorithm)
- Combinatorial enumerations
 (Lattice paths, Young tableaux, matching theory)

Hankel matrices over words

Let Σ be a finite alphabet and \mathcal{F} be a field and let $f: \Sigma^* \to \mathcal{F}$ be a function on words.

A finite or infinite matrix $H(f) = h_{u,v}$ indexed over the words $u, v \in \Sigma^*$ is a Hankel matrix for f if $h_{u,v} = f(u \circ v)$. Here \circ denotes concatenation.

Hankel matrices over words have applications in

- Formal language theory and stochastic automata,
 - J. Carlyle and A. Paz 1971
- Learning theory (exact learning of queries).
 A.Beimel, F. Bergadano, N. Bshouty, E. Kushilevitz, S. Varricchio 1998
 J. Oncina 2008
- Definability of picture languages.
 - O. Matz 1998, and D. Giammarresi and A. Restivo 2008

Multiplicity Automata

A Multiplicity Automaton (MA) A of size r is given by:

- A set $\{\mu_{\sigma} : \sigma \in \Sigma\}$ of $r \times r$ matrices over \mathcal{F} ;
- Two vectors $\lambda, \gamma \in \mathcal{F}^r$.
- A defines a function $f_A: \Sigma^* \to \mathcal{F}$

$$f_A(w) = f_A(\sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_n) = \lambda \mu_{\sigma_1} \mu_{\sigma_2} \cdot \ldots \cdot \mu_{\sigma_n} \gamma^t$$

THEOREM: (J. Carlyle and A. Paz 1971)

A function $f: \Sigma^* \to \mathcal{F}$ is representable as f_A for some MA A iff the Hankel matrix H(f) has finite rank.

Hankel matrices for graphs

If we want to define Hankel matrices for (labeled) graphs,

what plays the role of concatenation?

- Disjoint union
 Used by Freedman, Lovász and Schrijver, 2007, for characterizing multiplicative graph parameters over the real numbers
- k-unions (connections, connection matrices)
 Used by Freedman, Lovász, Schrijver and Szegedy, 2007ff, for characterizing various forms and partition functions.
- Joins, cartesian products, generalized sum-like operations used by Godlin, Kotek and JAM (2008) to prove non-definability.

The \square -rank of a property P

Given

- a binary operation \Box between structures $\mathfrak{A}(A,\bar{R},\bar{F},\bar{c})$ with relations \bar{R} , functions \bar{F} and constants \bar{c}), and no restrictions on their number of arguments, and
- a property P of such structures

we say that P has \square -rank $r(P\square) \in \mathbb{N} \cup \{\infty\}$ if $r(P\square) = rk(P,\square)$ is the rank of the Hankel matrix $\mathfrak{H}(P,\square)$ over the field \mathbb{Z}^2 .

\mathcal{L} -smooth operations.

Let \mathcal{L} be a logic with a well defined quantifier rank.

Here \mathcal{L} is one of **FOL**, MSOL, CMSOL.

We say that two graphs G, H are (\mathcal{L}, q) -equivalent, and write $G \sim_{\mathcal{L}}^q H$, if G and H satisfy the same \mathcal{L} -sentences of quantifier rank q.

We say that \square is \mathcal{L} -smooth, if whenever we have

$$G_i \sim^q_{\mathcal{L}} H_i, i = 0, 1$$

then

$$G_0 \square G_1 \sim_{\mathcal{L}}^q H_0 \square H_1$$

This definition can be adapted to k-graphs and also to structures with k-ary operations for $k \ge 1$.

Proving that an operation \square is \mathcal{L} -smooth

Proving that an operation \square is \mathcal{L} -smooth may be difficult.

For FOL, MSOL and CMSOL this can be achieved using

Ehrenfeucht-Fraïssé games also know as pebble games.

The case for MSOL was first proved by Hans Läuchli in 1966.

Anther way of establishing smoothness is via generalizations of the Feferman-Vaught theorem.

Makowsky, Johann A. "Algorithmic uses of the FefermanVaught theorem." Annals of Pure and Applied Logic 126.1-3 (2004): 159-213.

In this talk we need two cases:

 $\square = \sqcup$, the disjoint union, and $\square = Subst$, the substution of pointed graphs.

Theorem: (EF and JAM) Both \sqcup and Subst are CMSOL-smooth.

The Finite Rank Theorem

Theorem (Godlin, Kotek, Makowsky 2008):

Let f be a numeric graph parameter or graph polynomial for τ -structures definable in \mathcal{L} and taking values in an integral domain \mathcal{R} .

Let \square be an \mathcal{L} -smooth operation.

Then the connection matrix $M(f, \square)$ has finite rank over \mathcal{R} .

The **Proof** uses a Feferman-Vaught-type theorem for graph polynomials, due to B. Courcelle, J.A.M. and U. Rotics, 2000.

- C. Blatter and E. Specker prove it for Subst and MSOL.
- L. Lovasz proves it for patition functions.

It has many applications in graph theory.

Bounded U-rank and bounded degree

Theorem(EF and JAM, 2002)

Let P be a property of structures over some fixed vocabulary. If P has finite \sqcup -rank and all its members of are bounded degree d. Then

- $d_P^m(n)$ is ultimately periodic for every m.
- Furthermore, if additionally all the models in P are connected, $d_P^m(n) = 0$ for all m and n.

Example $d_{EQ_2}(n)$ shows that bounded degree cannot be dropped, even for \sqcup -rank 2 (and connected structures).

For structures of unbounded degree one needs a stronger assumption, the finiteness of the Subst-rank.

\sqcup -rank of \mathcal{P} and Gessel-classes

- A class of structures P is a Gessel class if for every $\mathfrak A$ and $\mathfrak B$, $\mathfrak A \sqcup \mathfrak B \in \mathcal P$ iff both $\mathfrak A \in \mathcal P$ and $\mathfrak B \in \mathcal P$.
- The class of forests is a Gessel class.
- If P is hereditary and closed under disjoint unions, it is a Gessel class.
- Every Gessel class has ⊔-rank at most 2.
- If $\mathcal P$ is a class of connected graphs, $\mathcal P$ has \sqcup -rank at most 2, but is not a Gessel class.
- If \mathcal{P}_1 and \mathcal{P}_2 have finite \sqcup -rank, so do $\mathcal{P}_1 \cup \mathcal{P}_2$, $\mathcal{P}_1 \cap \mathcal{P}_2$, and the complement $\bar{\mathcal{P}}_1$.

Gessel's Theorem (1984)

Theorem:(I. Gessel 1984)

If $\mathcal C$ is a Gessel class of directed graphs of degree at most d, then

$$d_{\mathcal{C}}(m+n) \equiv d_{\mathcal{C}}(m) \cdot d_{\mathcal{C}}(n) \pmod{\frac{m}{\ell}}$$

where ℓ is the least common multiple of all divisors of m not greater than d.

In particular, $d_{\mathcal{C}}(n)$ satisfies for every $m \in \mathbb{N}$ the linear recurrence relation

$$d_{\mathcal{C}}(n) \equiv a^{(m)} d_{\mathcal{C}}(n - d!m) \pmod{m}$$

where $a^{(m)} = d_{\mathcal{C}}(d!m)$.

Many classes of finite \sqcup -rank and Subst-rank.

There are only countably many classes of structures definable by CMSOL-formulas.

How many classes are there of finite ⊔-rank?

Proposition: (After an idea of Specker, 2002)

- (i) There are continuum many Gessel classes.
- (ii) There are continuum many properties of structures with ⊔-rank 2.
- (iii) There are continuum many properties of structures with finite Subst-rank.

File:sp-gessel 35

Relation between \sqcup -rank and Subst-rank

We denote by $G \bowtie H$ the join of G and H.

Proposition: Let P be a graph property. We have

- (i) $rk(P, \sqcup) \leq rk(P, Subst)$ and $rk(P, \bowtie) \leq rk(P, Subst)$.
- (ii) The class HAM of Hamiltonian graphs is connected, hence has \sqcup -rank 2, However, HAM has infinite \bowtie -rank, hence also infinite Subst-rank.

Problem: What can we say about $d_{HAM}^m(n)$?

Complexity

Let \mathcal{H} be a possible infinite set of finite graphs.

Let $F_{sub}(\mathcal{H})$, $(F_{ind}(\mathcal{H}), F_{min}(\mathcal{H}))$ be the class of finite graphs with forbidden subgraphs (induced subgraphs, minors) in \mathcal{H} .

If \mathcal{H} is finite they all have finite Subst-rank, because they are \mathbf{MSOL} , resp. **FOL** definable.

Problem:

- If \mathcal{H} is finite, what is the computational complexity of computing the Subst-rank of $F_{sub}(\mathcal{H})$, $(F_{ind}(\mathcal{H}), F_{min}(\mathcal{H}))$ measured in the size of \mathcal{H} ?
- In particular, what is the complexity if \mathcal{H} ? is a singleton?
- If \mathcal{H} is infinite, do $F_{sub}(\mathcal{H})$ and $F_{ind}(\mathcal{H})$ still have finite Subst-rank?

For $F_{min}(\mathcal{H})$, the answer is yes, due to the Robertson-Seymour Theorem, which states that every minor closed class of graphs is of the form $F_{min}(\mathcal{H})$ for some finite \mathcal{H} .

File:sp-gessel 37

Graph polynomials

Let F(G; x) be a univariate graph polynomial.

Examples: The chromatic polynomial, the independence polynomial, the matching polynomial, the characteristic polynomial, etc.

Let $G_n, n \in \mathbb{N}$ be a family of finite graphs and $a \in \mathbb{Z}$.

Let $f_{F,a}^m(n) = F(G_n; a) \mod m$.

The density function $d_P^m(n)$ for a graph property P is a special case where $G_n=E_n$ is the edge-free graph of order n, a=1 and

$$F_P(G; n) = \sum_{E \subseteq [n]^2 : ([n], E) \in P} x^{|E|}$$

Problem: When is the sequence $f_F^m(n)$ ultimately periodic?

39

The widely overlooked paper: its merits

- It initiates a systematic study of congruence relations for combinatorial counting functions.
 Before, and still now, mostly special cases are studied.
- It anticipates the use of the rank of Hankel matrices in combinatorics
 In the recent work of L. Lovász and his many collaborators on graph limits and partition functions this plays a central role.
- It formulates for the first time a meta-theorem connecting definability in MSOL with combinatorics. The Büchi-Elgot-Trakhtenbrot Theorem characterizes regular languages using MSOL. Bruno Courcelle and his collaborators use MSOL-definability to show that NP-hard problems are in P for graphs properties of bounded tree- and clique-width.

File:sp-conclu

The widely overlooked paper: Our improvements

- Eldar Fischer gave a counter example using a quaternary relation.
- Analyzing the counter example we noticed the role of bounded degree structures and the role of the ⊔-rank.
- Proving an earlier version of the Finite Rank Theorem for CMSOL we extended the Specker-Blatter Theorem to include Eulerian graphs (and many other cases).

File:sp-conclu 40

Thank you for your attention

Prof. emeritus J.A. Makowsky
Faculty of Computer Science
Technion - Israel Institute of Technology
Haifa, Israel

www.cs.technion.ac.il/~janos



janos@cs.technion.ac.il