FACULTY OF NATURAL, MATHEMATICAL & ENGINEERING SCIENCES

DEPARTMENT OF INFORMATICS

KING'S College LONDON

Formalising Mathematics to Obtain Verified AI and Optimisation Software

Thomas Ammer David Wang (supervised by Mohammad Abdulaziz)

A Motivation: Software and Hardware Failures

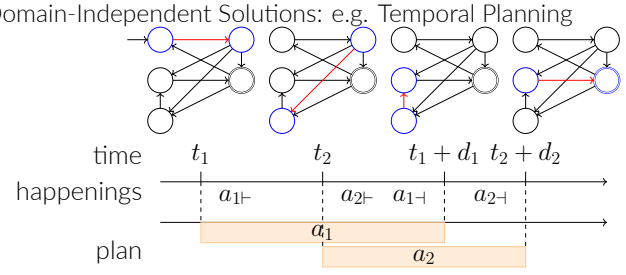
- Post Office Scandal(SF, > 900 postmasters wrongly convicted)
- Pentium FDIV (HF, flawed floating-point unit in processor)
- Therac-25 (SF, excessively high doses in radiation therapy)
- Boeing 737 (SF, screen blackouts when approaching specific runways, flight control)

Interactive Theorem Proving (ITP) and Isabelle

- Interactive Theorem Proving = Writing (partial) proofs s.t. they can be completed + checked by software
- Interactive Theorem Prover/Proof Assistant = Software to complete and check proofs
- We use Isabelle/HOL (others Coq/Rocq, Lean, etc.)
- Trustworthy Software
- In-depth understanding/explanation of behaviour

AI Planning

- See: https://formplan.github.io/
- Abstract Problem Representation: (1) Logic: e.g.
  $s \vDash \forall r{::}robot.\ \forall o{::}object.$
  $\text{weight}(o) \leq \text{capacity}(r) \wedge \neg\text{broken}(r) \wedge \ldots \longrightarrow \text{can\_carry}(r,o)$
  (2) Probabilities: e.g. Markov Decision Processes
- Domain-Independent Solutions: e.g. Temporal Planning

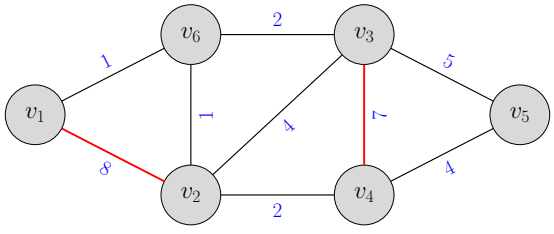


Find a schedule of concurrent actions that transform the initial state until a goal is satisfied. E.g. $s \vDash \forall x{::}task.\ \text{completed}(x)$

- Isabelle formalisation of a part of the Planning Domain Definition Language (PDDL) and its semantics based on abstract timed transition systems

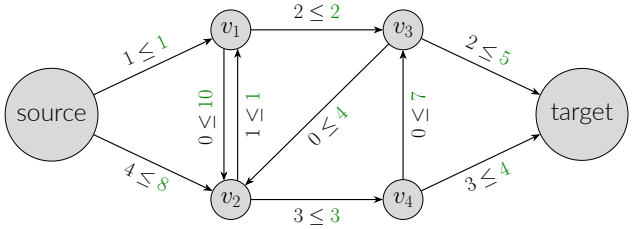
Examples for Combinatorial Optimisation (CO)

- Matching (certain one-to-one pairings allowed, selection from these, e.g. by Edmonds' Blossom Algorithm):



Combinatorial Optimisation (continued)

- Flows (send liquid from source to target while respecting connection capacities, e.g. by Ford-Fulkerson method):



Verifying Algorithms

- Planning and CO problems can be solved by algorithms
- Isabelle/HOL formalisation of mathematical theory to verify these algorithms
- Library for graph algorithms (together with collaborators): flows, matchings, matroids, spanning trees etc.
- Running Time: Time waiting for solution in relation to size of problem description
- Correctness guarantee for result if using verified code

Applications of Planning and CO Problems

Matching:

- Kidney Exchange in UK and Scandinavia [2, 8]
- Student-College Matching with preferences and fairness [1]
- Auctions and Market Design, e.g. Google's Adwords [17]

Flows:

- Electricity Grid Congestion, Pipe Network Analysis, and other transportation subject to capacities and costs
- Circuit and other Hardware Design. Esp. Very Large Scale Integration (VLSI), e.g. decrease of chip area by 23% [9], reduction of wire length by 10% [11], minimise cell movement [4], and others [5, 7, 13])

Planning:

- Logistics [20] (minimising costs of moving vessels), Enterprise Risk Management [19, 12] (e.g. Scenario Planning: i.e. modelling risk scenarios)
- Robotics [6], Space Exploration [14, 10, 15, 18] (e.g. optimising data up- and downlink times, providing reasoning capabilities to autonomous agents) + Terrestrial Exploration [16, 3] (e.g. improving returns of earth-observing satellites, guidance for autonomous underwater vehicles)

Further Remarks

Given the advantages of verification, also consider:

- Verification Effort vs. Increased Trustworthiness
- Unverified Assumptions (e.g. Compiler, Hardware)
- Good Running Time (thus high complexity) vs. Verification Effort
- for more info, go to https://fm-vs.github.io/

Formalising Mathematics to Obtain Verified AI and Optimisation Software: References

[1] Atila Abdulkadiroğlu. College admissions with affirmative action. *International Journal of Game Theory*, 33(4):535–549, Nov 2005.

[2] Péter Biró, Joris van de Klundert, David Manlove, William Pettersson, Tommy Andersson, Lisa Burnapp, Pavel Chromy, Pablo Delgado, Piotr Dworczak, Bernadette Haase, Aline Hemke, Rachel Johnson, Xenia Klimentova, Dirk Kuypers, Alessandro Nanni Costa, Bart Smeulders, Frits Spieksma, María O. Valentín, and Ana Viana. Modelling and optimisation in european kidney exchange programmes. *European Journal of Operational Research*, 291(2):447–456, 2021.

[3] Abigail Breitfeld, Alberto Candela, Juan Delfa, Akseli Kangaslahti, Itai Zilberstein, Steve Chien, and David Wettergreen. Learning-based planning for improving science return of earth observation satellites. In *Proceedings of the International Symposium on Artificial Intelligence, Robotics and Automation in Space*, 11 2024.

[4] Ulrich Brenner. Vlsi legalization with minimum perturbation by iterative augmentation. In *2012 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1385–1390, 2012.

[5] Ulrich Brenner, Anna Pauli, and Jens Vygen. Almost optimum placement legalization by minimum cost flow and dynamic programming. In *Proceedings of the 2004 International Symposium on Physical Design*, ISPD '04, page 2–9, New York, NY, USA, 2004. Association for Computing Machinery.

[6] Michael Cashmore, Maria Fox, Derek Long, Daniele Magazzeni, Bram Ridder, Arnau Carrera, Narcís Palomeras, Natàlia Hurtós, and Marc Carreras. Rosplan: Planning in the robot operating system. In *Proceedings International Conference on Automated Planning and Scheduling, ICAPS*, volume 2015-Janua, pages 333–341, 2015.

[7] Minsik Cho, Haoxing Ren, Hua Xiang, and Ruchir Puri. History-based vlsi legalization using network flow. In *Proceedings of the 47th Design Automation Conference*, DAC '10, page 286–291, New York, NY, USA, 2010. Association for Computing Machinery.

[8] Maxence Delorme, Sergio García, Jacek Gondzio, Jörg Kalcsics, David Manlove, William Pettersson, and James Trimble. Improved instance generation for kidney exchange programmes. *Computers & Operations Research*, 141:105707, 2022.

[9] K. Doll, F.M. Johannes, and K.J. Antreich. Iterative placement improvement by network flow methods. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 13(10):1189–1200, 1994.

[10] Tara Estlin, Gregg Rabideau, Darren Mutz, and Steve Chien. Using continuous planning techniques to coordinate multiple rovers. *Electronic Transactions on Artificial Intelligence*, 2000.

[11] Jia-Wei Fang, I-Jye Lin, Yao-Wen Chang, and Jyh-Herng Wang. A network-flow-based rdl routing algorithmz for flip-chip design. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 26(8):1417–1429, 2007.

[12] Mark Feblowitz, Oktie Hassanzadeh, Michael Katz, Shirin Sohrabi, Kavitha Srinivas, and Octavian Udrea. Ibm scenario planning advisor: A neuro-symbolic erm solution. In *35th AAAI Conference on Artificial Intelligence, AAAI 2021*, volume 18, 2021.

[13] Jiang Hu and Sachin S. Sapatnekar. A survey on multi-net global routing for integrated circuits. *Integration*, 31(1):1–49, 2001.

[14] Akseli Kangaslahti, Itai Zilberstein, Alberto Candela, and Steve Chien. Search applications for integrated planning and execution of satellite observations using dynamic targeting, 4 2025.

[15] Russell Knight, Gregg Rabideau, Steve Chien, Barbara Engelhardt, and Rob Sherwood. Casper: Space exploration through continuous planning. *IEEE Intelligent Systems*, 16, 2001.

[16] Somaiyeh MahmoudZadeh, David M.W Powers, Karl Sammut, Adham Atyabi, and Amirmehdi Yazdani. A hierarchal planning framework for auv mission management in a spatiotemporal varying ocean. *Computers and Electrical Engineering*, 67, 2018.

[17] Aranyak Mehta, Amin Saberi, Umesh Vazirani, and Vijay Vazirani. Adwords and generalized online matching. *J. ACM*, 54(5):22–es, October 2007.

[18] Nicola Policella, Henrique Oliveira, and Tero Siili. Skeyp: Ai applied to soho keyhole operations. In *Proceedings - 2009 3rd IEEE International Conference on Space Mission Challenges for Information Technology, SMC-IT 2009*, 2009.

[19] Shirin Sohrabi. Ai planning for enterprise: Putting theory into practice. In *IJCAI International Joint Conference on Artificial Intelligence*, volume 2019-August, 2019.

[20] Kevin Tierney, Amanda Coles, Andrew Coles, Christian Kroer, Adam M. Britt, and Rune Møller Jensen. Automated planning for liner shipping fleet repositioning. In *ICAPS 2012 - Proceedings of the 22nd International Conference on Automated Planning and Scheduling*, 2012.