Research Statement of Curtis Bright

Summary My research focuses on developing new efficient techniques for solving large search problems in computer science, particularly those from theoretical and applied mathematics. To this end, I've worked in the intersection of the fields of artificial intelligence, high performance computing, and symbolic computation to develop MathCheck, an award-winning system that has resolved many open problems from a variety of fields. The success of MathCheck has been achieved by combining two independently successful paradigms that have traditionally been separate—*satisfiability solving* (SAT) and *symbolic computation* using a computer algebra system (CAS).

This approach is effective because it combines the best of both the SAT and CAS worlds. SAT solvers are powerful search engines that can solve many important and difficult problems such as verifying the correctness of a microprocessor's design. Despite this power, SAT solvers do not perform well on problems that require sophisticated mathematics. On the other hand, computer algebra systems perform well on mathematical problems but are not optimized for searching. Many combinatorial problems that require both powerful search and mathematics have been out of reach of present algorithms—but the SAT+CAS paradigm has the potential to make such problems feasible. Because of the huge number of mathematical problems that stand to benefit from efficient search routines the SAT+CAS paradigm has recently received a significant amount of attention from academia and industry [2, 19]. Given my expertise in both SAT and CAS, I have been at the forefront of this movement, using the SAT+CAS paradigm to solve problems deemed too large to solve just a few years ago.

SAT+CAS The SAT+CAS method is still in its infancy, having only been first proposed in 2015 [1, 20]. Despite this, it has already had some great successes, including finding the smallest counterexample to the Williamson conjecture—a problem open since 1944 [8, 9]. A counterexample was found in 1993 but the smallest counterexample was unknown until MathCheck resolved the problem in 2016. MathCheck was also successful in constructing over 100,000 new Williamson matrices [10, 11, 13] in all even orders up to 70—prior to my work this had only been completed up to order 18. The SAT+CAS paradigm has also solved special cases of the Ruskey–Savage and

Norine conjectures [19], verified the complex Golay conjecture [14, 15], found three new counterexamples to a conjecture on good matrices [6], and constructed the largest best matrices that are currently known [7].

These results have appeared in some of the most prestigious artificial intelligence, automated reasoning, and symbolic computation journals and conferences. For example, my work appeared in the 2018 and 2019 Association for the Advancement of Artificial Intelligence (AAAI) conferences [6, 10]. In 2019 this conference had an acceptance rate of 16.2%. In fact, two of my publications were honoured by being *invited papers*—first at Computer Algebra and Scientific Computing [8] and second in the Journal of Automated Reasoning [19]. The varied conjectures and problems in which the SAT+CAS method has already found application speaks to its versatility and its great potential to push the state-of-the-art in many more applications for years to come.

Projective Geometry One extremely prominent non-existence result in combinatorics is the fact that there are no projective planes of order ten. This result has only been achieved using special-purpose search code written for a Cray supercomputer making it impossible to verify that the computation completed correctly but I have produced a verifiable certificate for a subcase of this non-existence result [4].

Experimental Number Theory In 2016, I solved the problem (open since 2000) of computing the set of minimal primes in many different bases [5] including all bases up to 16. In particular, I solved the problem in base 23 and showed that the largest minimal prime in base 23 has over a million digits when written in base 10. This number was the tenth largest known probable prime ever discovered at the time.

Algorithmic Number Theory I have also worked on developing new number theoretic algorithms. My first ISSAC paper [16] developed a new algorithm for solving a vector version of the *rational reconstruction* problem from computational number theory and as an undergraduate I developed a new method of solving Ramanujan's square equation that Noam Elkies called "even more elementary" than the previously known solution [3].

Information Theory My work has resulted in new theoretical advances in information theory. In particular, I constructed the first infinite family of odd-perfect quaternion sequences, the second infinite family of perfect quaternion sequences, and the first examples of Williamson matrices in all orders that are powers of two [12].

Industrial Collaboration I have had the pleasure of collaborating with Maplesoft, the developers of the computer algebra system Maple. I used my experience developing MathCheck to make Maple's chromatic number and maximum clique commands much more efficient—a number of benchmarks that could not be solved using the previous version of Maple in hours can now be solved in seconds [18].

Future Work I am currently working on improving the efficiency and verifiability of search methods for projective planes. In particular, the projective planes in order eleven have never been characterized and it is unknown if any projective planes of order twelve exist. They are widely conjectured to not exist but based on no theoretical evidence—it's just that no one has yet been able to construct one and the search space is enormous. Other conjectures from the literature that I've studied and for which I have a reasonable chance of producing new results involve weighing matrices, G-matrices, D-optimal designs, propus arrays, Hadamard matrices with 2 circulant cores, and Turyn sequences—there is no shortage of combinatorial problems that mathematicians and engineers care about where more powerful solvers can make a big impact.

We have just scratched the surface of the kinds of problems that can be solved by coupling powerful search, computer algebra, and high performance computing. Given the power of the SAT+CAS paradigm to make combinatorial search efficient for many industrial applications (especially where high-level mathematical reasoning is essential), I would like to apply my methods to problems involving circuit optimization, matrix multiplication optimization [17], graph algorithms, and cryptanalysis. Given the enormous number of digital electronic circuits produced every year, a search tool that could find more efficient ways of designing Boolean circuits would be worth hundreds of millions of dollars to the world's economy. As our search techniques become more powerful it excites me to think that one day when designing a electronic circuit a computer engineer may well use a SAT+CAS solver to find a more efficient implementation of that circuit.

Finally, I am currently writing an industrial collaboration grant with Maplesoft that will support research dedicated to improving the performance of Maple by using SAT solvers. My research developing SAT+CAS systems and effective SAT encodings of mathematical problems has been greatly beneficial while preparing this grant.

References

[1] E. Ábrahám. Building bridges between symbolic computation and satisfiability checking. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, pages 1–6. ACM, 2015.

[2] E. Ábrahám, J. Abbott, B. Becker, A. M. Bigatti, M. Brain, B. Buchberger, A. Cimatti, J. H. Dav-

enport, M. England, P. Fontaine, et al. SC^2: Satisfiability checking meets symbolic computation. *Intelligent Computer Mathematics: Proceedings CICM*, 9791:28–43, 2016.

[3] C. Bright. Solving Ramanujan's square equation computationally. `https://cs.uwaterloo.ca/~cbright/nsra/`, 2007.

[4] C. Bright, K. Cheung, B. Stevens, D. Roy, I. Kotsireas, and V. Ganesh. A verifiable search for projective planes of order ten. *Submitted*, 2019.

[5] C. Bright, R. Devillers, and J. Shallit. Minimal elements for the prime numbers. *Experimental Mathematics*, 25(3):321–331, 2016.

[6] C. Bright, D. Ž. Đoković, I. Kotsireas, and V. Ganesh. A SAT+CAS approach to finding good matrices: New examples and counterexamples. In *Thirty-Third AAAI Conference on Artificial Intelligence*. AAAI Press, 2019.

[7] C. Bright, D. Ž. Đoković, I. Kotsireas, and V. Ganesh. The SAT+CAS method for combinatorial search with applications to best matrices. *Submitted*, 2019.

[8] C. Bright, V. Ganesh, A. Heinle, I. Kotsireas, S. Nejati, and K. Czarnecki. MathCheck2: A SAT+CAS verifier for combinatorial conjectures. In *International Workshop on Computer Algebra in Scientific Computing*, pages 117–133. Springer, 2016.

[9] C. Bright, V. Ganesh, A. Heinle, I. Kotsireas, S. Nejati, and K. Czarnecki. MathCheck2: A SAT+CAS verifier for combinatorial conjectures. In *Proceedings of the 1st Workshop on Satisfiability Checking and Symbolic Computation*, pages 13–19, 2016.

[10] C. Bright, I. Kotsireas, and V. Ganesh. A SAT+CAS method for enumerating Williamson matrices of even order. In *Thirty-Second AAAI Conference on Artificial Intelligence*, pages 6573–6580. AAAI Press, 2018.

[11] C. Bright, I. Kotsireas, and V. Ganesh. The SAT+CAS paradigm and the Williamson conjecture. *ACM Communications in Computer Algebra*, 52(3):82–84, 2018.

[12] C. Bright, I. Kotsireas, and V. Ganesh. New infinite families of perfect quaternion sequences and Williamson sequences. *Submitted*, 2019.

[13] C. Bright, I. Kotsireas, and V. Ganesh. Applying computer algebra systems with SAT solvers to the Williamson conjecture. *Journal of Symbolic Computation*, to appear, 2019.

[14] C. Bright, I. Kotsireas, A. Heinle, and V. Ganesh. Complex Golay pairs up to length 28: A search via computer algebra and programmatic SAT. *Submitted*, 2018.

[15] C. Bright, I. Kotsireas, A. Heinle, and V. Ganesh. Enumeration of complex Golay pairs via programmatic SAT. In *Proceedings of the 2018 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2018, New York, NY, USA, July 16–19, 2018*, pages 111–118, 2018.

[16] C. Bright and A. Storjohann. Vector rational number reconstruction. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, pages 51–58. ACM, 2011.

[17] M. J. Heule, M. Kauers, and M. Seidl. Local search for fast matrix multiplication. *arXiv preprint arXiv:1903.11391*, 2019.

[18] Waterloo Maple Inc. Maple help documentation: What's new in Maple 2018.

[19] E. Zulkoski, C. Bright, A. Heinle, I. Kotsireas, K. Czarnecki, and V. Ganesh. Combining SAT solvers with computer algebra systems to verify combinatorial conjectures. *Journal of Automated Reasoning*, 58(3):313–339, 2017.

[20] E. Zulkoski, V. Ganesh, and K. Czarnecki. MathCheck: A math assistant via a combination of computer algebra systems and SAT solvers. In *International Conference on Automated Deduction*, pages 607–622. Springer, 2015.