Research Statement of Curtis Bright

I work on developing efficient search algorithms to solve mathematical problems through satisfiability checking and computer algebra—blurring the lines between the solvable and really hard problems. To this end, my research combines the fields of artificial intelligence, high performance computing, and symbolic computation, and has lead to the development of MathCheck, an award-winning system that has resolved a variety of previously open problems in mathematics. 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 advanced 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 methods—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 received a significant amount of attention from academia and industry [2, 20, 22]. 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 too large to solve just a few years ago [14].

SAT+CAS The SAT+CAS method is still in its infancy, having only been first proposed in 2015 [1, 24]. Despite this, it has already had some great successes, including finding the smallest counterexample of the Williamson conjecture—a problem that was open since 1944 [10]. I used MathCheck to construct over 100,000 new Williamson matrices [12, 13, 15] in all even orders up to 70—prior to my work exhaustive searches had only been completed up to order 18. MathCheck has also been used to solve new cases of the Ruskey–Savage and Norine conjectures from 1993 and 2008 [23], verified conjectures of Craigen, Holzmann, and Kharaghani from 2002 [17, 18], found three new counterexamples to a conjecture on good matrices (first studied in 1971) [8], and constructed the largest currently known best matrices (first studied in 2001) [9].

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 [8, 12] (having an acceptance rate of around 16%). Two of my publications were also honoured by being *invited papers*—first

at Computer Algebra and Scientific Computing [10] and second in the Journal of Automated Reasoning [23].

Recently, I have been applying MathCheck to verify the solution of *Lam's Problem* (studied since the 1800s and solved in 1989) of showing that projective planes of order ten do not exist. So far, this result has only been achieved using special-purpose search code that is difficult to write and even more difficult to verify. In 2011, a verification of a subcase of Lam's problem required 16,000 hours of computing. MathCheck is able to complete the verification of this subcase in just 30 hours [4], and additionally produces a certificate that allows the result to be verified by an independent third party [5, 6]. 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.

Algorithmic Number Theory In 2016, I solved the problem (open since 2000) of computing the set of minimal primes in many different bases [7] including all bases up to 16. In particular, I solved the problem in base 23, showing 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.

Furthermore, my first ISSAC paper developed a new algorithm for solving a vector version of the rational reconstruction problem from computational number theory [19]. I also 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 proof that Williamson matrices exist in all orders that are powers of two [16].

Future and Current Research

My current and upcoming plans focus on improving the SAT+CAS method and extending its application to new problem domains. Currently, I am working on improving the ability of MathCheck to produce nonexistence certificates, using as a case study the domain of finite geometry. Certificates are particularly important in this field, as many prominent results (such as the solution of Lam's problem) rely on computer searches that have never been verified. Additionally, many problems in finite geometry are begging to be solved: the projective planes in order eleven have never been characterized, and it is unknown if any projective planes of order twelve exist. Other conjectures from the literature where the SAT+CAS method stands a good 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.

I believe 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 applications (especially where sophisticated mathematical calculations are essential), I plan to apply my methods to problems such as analyzing cryptosystems, circuit optimization, and graph theory problems like characterizing the strongly regular graphs. 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 [21]. 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 plan to continue exploring industrial applications of combining computer algebra and SAT solvers. As an example, I have worked with Maplesoft (the developers of the computer algebra system Maple) who supported research dedicated to improving the performance of discrete optimization routines in Maple. My research has already been greatly beneficial in this collaboration, resulting in dramatically improved versions of Maple's chromatic number and maximum clique commands. A number of benchmarks that could not be solved using the previous version of Maple in hours can now be solved in seconds [11].

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, 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. Searching for projective planes with computer algebra and SAT solvers. In *25th Conference on Applications of Computer Algebra*, 2019.

[5] C. Bright, K. Cheung, B. Stevens, D. Roy, I. Kotsireas, and V. Ganesh. A nonexistence certificate for projective planes of order ten with weight 15 codewords. *Applicable Algebra in Engineering, Communication and Computing*, 31:195–213, 2020.

[6] C. Bright, K. K. H. Cheung, B. Stevens, I. Kotsireas, and V. Ganesh. Nonexistence certificates for ovals in a projective plane of order ten. *Proceedings of the 31st International Workshop on Combinatorial Algorithms*, pages 97–111, 2020.

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

[8] 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*, pages 1435–1442. AAAI Press, 2019.

[9] C. Bright, D. Ž. Đoković, I. Kotsireas, and V. Ganesh. The SAT+CAS method for combinatorial search with applications to best matrices. *Annals of Mathematics and Artificial Intelligence*, 87(4):321–342, 2019.

[10] 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 18th International Workshop on Computer Algebra in Scientific Computing*, pages 117–133. Springer, 2016.

[11] C. Bright, J. Gerhard, I. Kotsireas, and V. Ganesh. Effective problem solving using SAT solvers. In *Maple in Mathematics Education and Research*, volume 1125 of *Communications in Computer and Information Science*, pages 205–219. Springer, Cham, 2020.

[12] 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.

[13] 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.

[14] C. Bright, I. Kotsireas, and V. Ganesh. SAT solvers and computer algebra systems: A powerful combination for mathematics. *Proceedings of the 29th International Conference on Computer Science and Software Engineering*, pages 323–328, 2019.

[15] C. Bright, I. Kotsireas, and V. Ganesh. Applying computer algebra systems with SAT solvers to the Williamson conjecture. *Journal of Symbolic Computation*, 100:187–209, 2020.

[16] C. Bright, I. Kotsireas, and V. Ganesh. New infinite families of perfect quaternion sequences and Williamson sequences. *IEEE Transactions on Information Theory*, 66(12):7739–7751, 2020.

[17] C. Bright, I. Kotsireas, A. Heinle, and V. Ganesh. Enumeration of complex Golay pairs via programmatic SAT. In *Proceedings of the 43rd International Symposium on Symbolic and Algebraic Computation, ISSAC 2018*, pages 111–118, 2018.

[18] C. Bright, I. Kotsireas, A. Heinle, and V. Ganesh. Complex Golay pairs up to length 28: A search via computer algebra and programmatic SAT. *Journal of Symbolic Computation*, 102:153–172, 2021.

[19] 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.

[20] J. H. Davenport, M. England, A. Griggio, T. Sturm, and C. Tinelli. Symbolic computation and satisfiability checking. *Journal of Symbolic Computation*, 100:1–10, 2020.

[21] A. B. Kahng, J. Lienig, I. L. Markov, and J. Hu. *VLSI Physical Design: From Graph Partitioning to Timing Closure*. Springer, 2011.

[22] D. Kaufmann, A. Biere, and M. Kauers. Verifying large multipliers by combining SAT and computer algebra. In *Proceedings of Formal Methods in Computer-Aided Design*, 2019.

[23] 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.

[24] 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.