Extended Research Statement of Curtis Bright

March 20, 2019

1 Introduction

A huge number of problems from theoretical and applied mathematics require efficient techniques for searching through enormous spaces. My research has focused on developing new efficient techniques for solving these problems. To this end I've worked in the intersection of the fields of automated reasoning and symbolic computation developing MathCheck, an award-winning system that has resolved many open problems from a variety of fields of mathematics (see `uwaterloo.ca/mathcheck`). The success of MathCheck has been achieved by combining state-of-the-art tools for satisfiability checking (SAT solvers) with computer algebra systems (CAS). This "SAT+CAS" approach has recently received a significant amount of attention from academia and industry [1] and 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.

The SAT+CAS approach is particularly exciting because of the huge number of applications that could benefit from efficient combinatorial search routines. For example, 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. The problem of "minimizing" a Boolean circuit is so difficult that it is often dismissed out of hand but recently SAT solvers have made progress on this important problem [35]. 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.

2 MathCheck Results

I am the lead developer of the SAT+CAS system MathCheck and have used it to solve many open conjectures from combinatorial design theory, number theory, and graph theory. In the process of solving these conjectures a number of interesting new combinatorial objects were explicitly constructed. Even more interestingly, my examination of these new objects revealed new properties and conjectures that were previously unknown.

2.1 Hadamard Matrices

As an example, consider the problem of finding *Hadamard matrices*—square matrices whose entries are 1 or -1 and whose rows are pairwise orthogonal. Such matrices have been studied for over 150 years we still don't know of a guaranteed practical method that can construct a Hadamard matrix of a given size. Not for a lack of trying; such an algorithm would be extremely useful as Hadamard matrices have applications to error-correcting codes [44], image coding [47], and techniques for statistical estimation [48]. As a part of my research I've constructed over 100,000 new Hadamard matrices of various kinds [15], including many constructed from Williamson, good, and best matrices (see below).

2.2 Williamson Matrices

In 1944, John Williamson defined a class of matrices that can be used to construct Hadamard matrices [59]. They are now known as *Williamson matrices* and have since been studied for many applications, including by NASA scientists in the early 1960s when developing codes for communicating with space probes [29]. These scientists successfully constructed Williamson matrices in many small orders and conjectured that Williamson matrices exist in each order n. This conjecture was disproven in 1993 when the counterexample $n = 35$ was found [22] but it was unknown if this was the smallest counterexample until MathCheck verified it in 2016 [12, 60]. I also showed for the first time that a generalization of Williamson matrices known as 8-Williamson matrices *do* exist for $n = 35$ [14].

Prior to my work, Williamson matrices had only been enumerated in the odd orders $n \leq 61$ [32, 40] and the even orders $n \leq 18$ [37]. Using MathCheck I increased the orders that have been enumerated to all $n \leq 70$ except $n = 65$ and $n = 67$ [14]. I found that Williamson matrices exist in all even orders $n \leq 70$, leading to the new conjecture that Williamson matrices exist in all even orders.

These new results were made possible not only because of the power of MathCheck but new theoretical properties of Williamson matrices that I discovered

while studying the structure of Williamson matrices. For example, I proved a product theorem that the entries of Williamson matrices of even order must satisfy [6]. Such a theorem was proven by Williamson in the odd order case in 1944, but the theorem had never been generalized to even orders. Additionally, I found a simple construction from which one can construct Williamson matrices of order $2n$ using Williamson matrices of odd order n [7] and a construction for 8-Williamson matrices of odd order n from Williamson matrices of order $2n$ [13].

2.3 Good and Best Matrices

The classes of matrices known as good and best matrices were defined in 1970 and 2001 respectively [54, 27] in order to construct Hadamard matrices whose off-diagonal entries are anti-symmetric. It is known that if good matrices exist in order n then n must be odd and if best matrices exist in order n then n must be of the form $r^2 + r + 1$. Both of these necessary conditions were conjectured to be sufficient and an enumeration performed in 2018 [23] for orders $n \leq 49$ showed that the best matrix conjecture holds for all $r \leq 6$ but the good matrix conjecture fails for $n = 41$, 47, and 49.

Using MathCheck, I found three new counterexamples ($n = 51$, 63, and 69) to the good matrix conjecture and found new examples of good matrices in the orders $n = 27$ and 57 [10]. I also showed that the best matrix conjecture holds for $r = 7$ for the first time by constructing three sets of best matrices of order 57—the largest best matrices that are currently known [11].

2.4 Complex Golay Pairs

Complex Golay pairs are a pair (A, B) of polynomials with coefficients in $\{\pm 1, \pm i\}$ and of degree $n - 1$ such that $|A(z)|^2 + |B(z)|^2 = 2n$ for all z on the unit circle. These polynomials (with real coefficients) were first used by Golay to solve a problem in infrared multislit spectrometry [28] and have since been applied to an enormous number of engineering applications such as in communications [52]. They also provide extremal examples for various problems in number theory [3]. Based on a partial search they were conjectured to not exist for $n = 23$ [20]. Using MathCheck I independently verified the confirmation of this conjecture by [25] and made available a complete enumeration of complex Golay pairs for $n \leq 28$ for the first time [16, 17].

3 Other Results

Despite the success of the SAT+CAS paradigm it is not appropriate for all kinds of problems. Given this, I have solved other problems using techniques more appropriate to the problem at hand.

3.1 Minimal Prime Numbers

In 2000, Jeff Shallit proved the amazing fact [50] that *every* prime number when expressed in base 10 contains one of the following primes as a subword:

$$\{2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991, 6469, 6949, 9001,$$
$$9049, 9649, 9949, 60649, 666649, 946669, 60000049, 66000049, 66600049\}$$

For example, the prime 4909 contains 409 as a subword. This set is known as the *minimal* primes in base 10 because these primes form the smallest set of primes that have this magical property. However, the set of minimal primes is dependent on the base that the primes are represented in and he left open the problem of determining the minimal primes in bases other than 10.

This problem is especially difficult because although the set of minimal primes is known to be finite there is no known upper bound on its size, i.e., the search space is infinite. Despite this, I wrote a special-purpose solver (using sophisticated search and filtering algorithms) that solved the problem in many small bases including all bases up to 16. The numbers involved became enormous, requiring the usage of special-purpose primality checking programs—in fact, the numbers were so large that *probable* primality tests had to be used. For example, my program solved the problem in base 23 and the largest minimal prime in base 23 has over a million digits when written in base 10. It was the tenth largest known probable prime ever discovered at the time it was found [9].

3.2 Vector Rational Reconstruction

I have also worked on developing new number theoretic algorithms. In particular, I developed a new algorithm for solving a vector version of the *rational reconstruction* problem from computational number theory. In other words the problem of finding small solutions $x_1, \ldots, x_n, y$ to the simultaneous congruences

$$yc_i \equiv x_i \pmod{M} \qquad \text{for } i = 1, \ldots, n$$

where $c_1, \ldots, c_n, M$ are given.

It is known from elementary number theory that if the entries in the solution are absolutely bounded by N and $M > 2N^2$ then there is a simple efficient

algorithm for solving this problem and the solution is unique if it exists. However, in many applications of interest (such as when linear system solving using a modular algorithm [45]) the solution will be unique even when M is much smaller than $2N^2$—but the simple algorithm cannot be used in these cases because it requires that $M > 2N^2$. I developed an efficient algorithm that finds the solution with weaker bounds on M. In particular, my algorithm only requires that $M > 4N^{4/3}$ [18].

3.3 Industrial Collaboration

As a postdoctoral researcher I have had two research internships with Maplesoft, the distributors of the computer algebra system Maple. During these internships I improved the performance of Maple's Satisfy, ChromaticNumber, and MaximumClique commands. Satisfy solves a SAT instance, ChromaticNumber computes the *chromatic number* of a graph and MaximumClique computes the *maximum clique* in a graph.

Satisfy was improved by updating the variable branching heuristic used by the SAT solver [42] and eliminating overhead in the CAS–SAT interface. These improvements meant that SAT solving was now fast enough to be used as a subroutine in other commands. I used my experience developing MathCheck to reduce the chromatic number and maximum clique problems to SAT and then solved them using Satisfy. In each case this approach performed better on average than the previous approach used by Maple. In fact, a number of benchmarks that could not be solved using the previous version of Maple in hours can now be solved in seconds [55].

Additionally, I wrote a number of reports explaining in detail how many interesting mathematical problems can be solved by reducing them to a SAT problem. These worksheets have been published by Maplesoft as a collection of Maple worksheets [56].

4 Future Work

Although it is necessarily difficult to predict where research will lead there are a number of possible extensions of my work that I am currently exploring and interested in pursuing in more depth.

4.1 Finite Projective Planes

Projective geometry has been studied by mathematics, engineers, and artists for over 500 years. A geometry is *projective* if any two lines intersect in some

point, i.e., if parallel lines do not exist. A geometry is *finite* if a finite number of points exist. For many years it has been known that finite geometries exist in all orders that are prime powers but it is still unknown if finite projective planes exist in other orders.

In 1782 Euler studied *Eulerian squares* that are a necessary substructure of any finite projective plane [24]. Euler found a way to construct these squares in any order that is not of the form $4k + 2$. It is not possible to construct them in order two and he could not construct them in orders six or ten, leading him to conjecture that Eulerian squares, and hence projective planes, do not exist in orders of the form $4k + 2$.

Euler's conjecture became famous as Euler was not able to resolve it during his life. The first progress on the conjecture did not come until 1900 when Tarry showed Eulerian squares do not exist in order six [53]. This gave evidence to Euler's conjecture and subsequently Peterson (1901) [46], Wernicke (1910) [57], and MacNeish (1922) [43] published erroneous proofs of the conjecture. Then, in 1959–1960 Bose, Shrikhande, and Parker published spectacular papers [4, 5] showing that Eulerian squares exist for all orders of the form $4k + 2$ except for two and six.

This raised the possibility that projective planes could also exist in those orders. A theorem of Bruck and Ryser from 1949 showed that certain orders were impossible, but left open other orders like ten and twelve. In the 1970s coding theory shed light on the structure that a projective plane of order ten must satisfy but mathematicians were still unable to construct them. In the 1980s, Prof. Clement Lam of Concordia University realized that with the advancements in coding theory and computing power it was just feasible for a supercomputer to complete a search for a projective plane of order ten. After about a decade of work, in 1991 Lam finally announced [39] that his search had determined that no projective planes exist in order ten.

In 2002, Dominque Roy started a verification of Lam's search using off-the-shelf computers and began a parallel verification [49]. Even with the advances in technology it required 8 years for the computers to complete the search. However, neither search produced either a *formal verification* or *certificate* of the non-existence result.

Although such a task is a formidable challenge I have used SAT solvers to efficiently produce a certificate for a subcase of the non-existence result [8]. Solving the remaining cases will likely require sophisticated symmetry detection which is difficult for SAT solvers—fortunately, computer algebra systems excel at this task making the SAT+CAS paradigm perfectly suited to produce a non-existence certificate.

A formal verification would be much more difficult but the certificate pro-

duced by the SAT solver could be used as a first step. This approach has recently successfully solved the Boolean Pythagorean triples problem [31]. A formal verification was achieved by formally reducing the problem to SAT, using a SAT solver to produce a non-existence certificate, and then formally verifying the certificate in a theorem prover [21].

The SAT encoding is more straightforward in the Boolean Pythagorean triples problem but the same approach could be used to formally verify the non-existence of a projective plane of order ten. Even just generating a non-existence certificate using a SAT solver would be useful—then only the code that generates an encoding needs to be trusted, instead of code that performs a search. This is particularly important considering that search code usually has to be written in a convoluted way to achieve optimal performance.

The verification work in order ten should also be useful when solving larger orders—in particular, the projective planes of order eleven have not been characterized and it is unknown if any projective planes of order twelve exist. This problem is expected to be much harder than the order ten case. For example, there are three essential subcases in the order ten case but sixteen subcases in the order twelve case [30]. These subcases could each be orders of magnitude harder to solve than the order ten case but it is at least worth attempting to see how many (if any) can be solved.

Additionally, there is still the possibility of getting lucky and finding a projective plane of order twelve. Such a result would be explosive news and of interest even to non-mathematicians. For example, when Bose, Shrikhande, and Parker found a Eulerian square of order ten (thereby disproving Euler's 1782 conjecture) their result appeared on the front page of the New York Times. Similarly, Lam's result on the non-existence of projective planes of order ten was also covered by the New York Times.

4.2 Combinatorial Matrices and Sequences

As shown in Section 2 the SAT+CAS paradigm has solved a number of open problems in combinatorial design theory and constructed a number of new Hadamard matrices using Williamson, good, and best matrices. There are a number of directions in which this work could be extended.

Firstly, the SAT+CAS paradigm can be applied to verify (or counterexample) other conjectures and to construct other kinds of combinatorial matrices—there is no shortage of alternate constructions. Some of the matrices from the combinatorial literature that I've studied and where the SAT+CAS paradigm has a reasonable chance of producing new results include weighing matrices, G-matrices, propus matrices, Hadamard matrices with 2 circulant cores, and

Turyn sequences.

Secondly, we could extend our previous method and apply it to larger orders. For example, $n = 65$ is currently the smallest order for which it is unknown if Williamson matrices of order n exist or not. During some preliminary experimentation I split the search space for this order into about half a billion subcases such that each case can be solved in about a minute. In principle this could be solved with enough computing horsepower but it would also be prudent to examine the subcases in detail to see if some can be simplified further and to examine if alternate ways of splitting the search space yield even better search performance.

Thirdly, we can examine the combinatorial objects that we found to look for properties that could then be exploited to construct larger examples of these objects. For example, recently Acevedo and Dietrich discovered a link between Williamson matrices and perfect quaternionic sequences [2]. Their construction is very powerful and can be used to construct Williamson matrices of order 70. A year prior this would have solved an open problem, but MathCheck had already successfully completed a search for Williamson matrices of order 70 [15]. Their method also only produces *some* of the Williamson matrices of order 70 found by MathCheck. It would be interesting to see if their method could be extended to produce all Williamson matrices of order 70.

4.3 Improving Matrix Multiplication

On at least four occasions after presenting my work on SAT+CAS someone has approached me to suggest that I try to use MathCheck to find better matrix multiplication algorithms. This problem has a long history dating back to Strassen in 1969 who found an algorithm for multiplying 2×2 matrices using seven multiplications [51] and it was quickly shown that this result was optimal [33]. In the 1970s algorithms for multiplying 3×3 matrices were found that used twenty-five [26], twenty-four [34], and finally twenty-three [38] multiplications.

For 35 years no further improvements in the 3×3 case were made but in 2012 a second algorithm also using twenty-three multiplications was found by reducing the problem to a SAT instance [19]. This approach appears to have reached a limit, however, as the SAT instances generated through this reduction are known to be extremely difficult to solve and much computation time has already been spent trying to solve them [36]. The SAT+CAS paradigm, with its powerful ability to detect symmetries and remove isomorphisms (symmetry breaking) has the potential to push the state-of-the-art and either find a better 3×3 matrix multiplication algorithm or show that one does not exist.

In general $n \times n$ matrix multiplication is said to be solvable in $O(n^\omega)$ time where $\omega < 2.3729$ and much effort has been spent trying to reduce this bound [41]. Williams points out [58] that one reason why determining the complexity of matrix multiplication is difficult is because optimal algorithms for multiplying small matrices are still unknown. Algorithms for general matrix multiplication rely on a divide and conquer approach so a better algorithm for multiplying small matrices has the potential to improve general matrix multiplication as well.

References

[1] Erika Ábrahám, John Abbott, Bernd Becker, Anna M Bigatti, Martin Brain, Bruno Buchberger, Alessandro Cimatti, James H Davenport, Matthew England, Pascal Fontaine, et al. SC^2: Satisfiability checking meets symbolic computation. *Intelligent Computer Mathematics: Proceedings CICM*, 9791:28–43, 2016.

[2] Santiago Barrera Acevedo and Heiko Dietrich. New infinite families of Williamson Hadamard matrices. *Australasian Journal of Combinatorics*, 73(1):207–219, 2019.

[3] Peter Borwein. Barker polynomials and Golay pairs. In *Computational Excursions in Analysis and Number Theory*, CMS Books in Mathematics, pages 109–119. Springer-Verlag New York, 2002.

[4] Raj Chandra Bose, Sharadchandra S Shrikhande, and Ernest T Parker. Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. *Canadian Journal of Mathematics*, 12:189–203, 1960.

[5] Raj Chandra Bose and Sharadchandra Shankar Shrikhande. On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order $4t + 2$. *Proceedings of the National Academy of Sciences of the United States of America*, 45(5):734, 1959.

[6] Curtis Bright. A new form of Williamson's product theorem. *arXiv preprint arXiv:1711.07056*, 2017.

[7] Curtis Bright. A doubling construction for Williamson matrices. *arXiv preprint arXiv:1803.01480*, 2018.

[8] Curtis Bright, Kevin Cheung, Brett Stevens, Dominique Roy, Ilias Kotsireas, and Vijay Ganesh. A verifiable search for projective planes of order ten. *In submission*, 2019.

[9] Curtis Bright, Raymond Devillers, and Jeffrey Shallit. Minimal elements for the prime numbers. *Experimental Mathematics*, 25(3):321–331, 2016.

[10] Curtis Bright, Dragomir Ž Đoković, Ilias Kotsireas, and Vijay Ganesh. A SAT+CAS approach to finding good matrices: New examples and counterexamples. In *Thirty-Third AAAI Conference on Artificial Intelligence*. AAAI Press, 2019.

[11] Curtis Bright, Dragomir Ž Đoković, Ilias Kotsireas, and Vijay Ganesh. The SAT+CAS method for combinatorial search with applications to best matrices. *In submission*, 2019.

[12] Curtis Bright, Vijay Ganesh, Albert Heinle, Ilias Kotsireas, Saeed Nejati, and Krzysztof Czarnecki. MathCheck2: A SAT+CAS verifier for combinatorial conjectures. In *International Workshop on Computer Algebra in Scientific Computing*, pages 117–133. Springer, 2016.

[13] Curtis Bright, Ilias Kotsireas, and Vijay 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.

[14] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. The SAT+CAS paradigm and the Williamson conjecture. *ACM Communications in Computer Algebra*, 52(3):82–84, 2018.

[15] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. Applying computer algebra systems with SAT solvers to the Williamson conjecture. *To appear in the Journal of Symbolic Computation (subject to minor revisions)*, 2019.

[16] Curtis Bright, Ilias Kotsireas, Albert Heinle, and Vijay Ganesh. Complex Golay pairs up to length 28: A search via computer algebra and programmatic SAT. *In submission*, 2018.

[17] Curtis Bright, Ilias Kotsireas, Albert Heinle, and Vijay 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.

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

[19] Nicolas T Courtois, Daniel Hulme, and Theodosis Mourouzis. Multiplicative complexity and solving generalized Brent equations with SAT solvers. *Computation Tools*, 2012:22–27, 2012.

[20] Robert Craigen, W Holzmann, and Hadi Kharaghani. Complex Golay sequences: Structure and applications. *Discrete mathematics*, 252(1-3):73–89, 2002.

[21] Luís Cruz-Filipe, Joao Marques-Silva, and Peter Schneider-Kamp. Formally verifying the solution to the Boolean Pythagorean triples problem. *Journal of Automated Reasoning*, Oct 2018.

[22] Dragomir Ž Đoković. Williamson matrices of order $4n$ for $n = 33$, 35, 39. *Discrete mathematics*, 115(1-3):267–271, 1993.

[23] Dragomir Ž Đoković and Ilias S Kotsireas. Goethals–Seidel difference families with symmetric or skew base blocks. *Mathematics in Computer Science*, 12(4):373–388, 2018.

[24] Leonhard Euler. Recherches sur un nouvelle espéce de quarrés magiques. *Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen*, pages 85–239, 1782.

[25] Frank Fiedler. Small Golay sequences. *Advances in Mathematics of Communications*, 7(4), 2013.

[26] N Gastinel. Sur le calcul des produits de matrices. *Numerische Mathematik*, 17(3):222–229, 1971.

[27] S Georgiou, C Koukouvinos, and Jennifer Seberry. On circulant best matrices and their applications. *Linear and Multilinear Algebra*, 48(3):263–274, 2001.

[28] Marcel JE Golay. Multi-slit spectrometry. *JOSA*, 39(6):437–444, 1949.

[29] Solomon W Golomb and Leonard D Baumert. The search for Hadamard matrices. *The American Mathematical Monthly*, 70(1):12–17, 1963.

[30] Marshall Hall Jr and John Wilkinson. Ternary and binary codes for a plane of order 12. *Journal of Combinatorial Theory, Series A*, 36(2):183–203, 1984.

[31] Marijn JH Heule, Oliver Kullmann, and Victor W Marek. Solving and verifying the Boolean Pythagorean triples problem via cube-and-conquer. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 228–245. Springer, 2016.

[32] Wolf H Holzmann, Hadi Kharaghani, and Behruz Tayfeh-Rezaie. Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 46(3):343–352, 2008.

[33] John E Hopcroft and Leslie R Kerr. Some techniques for proving certain simple programs optimal. In *10th Annual Symposium on Switching and Automata Theory (SWAT 1969)*, pages 36–45. IEEE, 1969.

[34] John E Hopcroft and Leslie R Kerr. On minimizing the number of multiplications necessary for matrix multiplication. *SIAM Journal on Applied Mathematics*, 20(1):30–36, 1971.

[35] Matti Järvisalo, Petteri Kaski, Mikko Koivisto, and Janne H Korhonen. Finding efficient circuits for ensemble computation. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 369–382. Springer, 2012.

[36] Manuel Kauers. No news on matrix multiplication. *Milestones in Computer Algebra*, 2016.

[37] Ilias S Kotsireas and Christos Koukouvinos. Constructions for Hadamard matrices of Williamson type. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 59:17–32, 2006.

[38] Julian D Laderman. A noncommutative algorithm for multiplying 3×3 matrices using 23 multiplications. *Bulletin of the American Mathematical Society*, 82(1):126–128, 1976.

[39] Clement WH Lam. The search for a finite projective plane of order 10. *The American mathematical monthly*, 98(4):305–318, 1991.

[40] Wolfgang Lang and Ekkehard Schneider. Turyn type Williamson matrices up to order 99. *Designs, Codes and Cryptography*, 62(1):79–84, Jan 2012.

[41] François Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th international symposium on symbolic and algebraic computation*, pages 296–303. ACM, 2014.

[42] Jia Hui Liang, Hari Govind VK, Pascal Poupart, Krzysztof Czarnecki, and Vijay Ganesh. An empirical study of branching heuristics through the lens of global learning rate. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 119–135. Springer, 2017.

[43] Harris F MacNeish. Euler squares. *Annals of Mathematics*, pages 221–227, 1922.

[44] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[45] Michael T McClellan. The exact solution of systems of linear equations with polynomial coefficients. In *Proceedings of the second ACM symposium on Symbolic and algebraic manipulation*, pages 399–414. ACM, 1971.

[46] J Peterson. Les 36 officieurs. *Ann. Math.*, 1:413–427, 1901.

[47] William K Pratt, Julius Kane, and Harry C Andrews. Hadamard transform image coding. *Proceedings of the IEEE*, 57(1):58–68, 1969.

[48] JNK Rao and Jun Shao. On balanced half-sample variance estimation in stratified random sampling. *Journal of the American Statistical Association*, 91(433):343–348, 1996.

[49] Dominique J Roy. Confirmation of the non-existence of a projective plane of order 10. Master's thesis, Carleton University, 2011.

[50] Jeffrey Shallit. Minimal primes. *Journal of Recreational Mathematics*, 30(2):113–117, 2000.

[51] Volker Strassen. Gaussian elimination is not optimal. *Numerische mathematik*, 13(4):354–356, 1969.

[52] Mohsen Taghavi and Mohsen Zahraei. On the autocorrelations of ± 1 polynomials. *Journal of Mathematical Extension*, 1(2):139–147, 2007.

[53] Gaston Tarry. *Le problème des 36 officiers*. Secrétariat de l'Association française pour l'avancement des sciences, 1900.

[54] Jennifer Seberry Wallis. *Combinatorial matrices*. PhD thesis, La Trobe University, 1970.

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

[56] Waterloo Maple Inc. Applications by Curtis Bright. `https://www.maplesoft.com/applications/Author.aspx?mid=345070`, 2018.

[57] P Wernicke. Das problem der 36 offiziere. *Jahresbericht der deutschen Mathematiker-Vereinigung*, 19:264–267, 1910.

[58] Ryan Williams. Applying practice to theory. *SIGACT News*, 39(4):37–52, November 2008.

[59] John Williamson. Hadamard's determinant theorem and the sum of four squares. *Duke Mathematical Journal*, 11(1):65–81, 1944.

[60] Edward Zulkoski, Curtis Bright, Albert Heinle, Ilias Kotsireas, Krzysztof Czarnecki, and Vijay Ganesh. Combining SAT solvers with computer algebra systems to verify combinatorial conjectures. *Journal of Automated Reasoning*, 58(3):313–339, 2017.