Designs, Codes and Cryptography (2022) 90:2517–2527
https://doi.org/10.1007/s10623-022-01126-z

Guest editorial: On coding theory and combinatorics—in memory of Vera Pless

W. Cary Huffman[1] · Jon-Lark Kim[2] · Patrick Solé[3]

Accepted: 22 September 2022 / Published online: 21 October 2022

This special issue of *Designs, Codes and Cryptography* is dedicated to Vera Stepen Pless, our beloved collaborator, advisor, and friend. Accounts of her biography and bibliography have appeared in several places [4, 20, 28, 29, 67]. The topics of the articles that comprise the issue reflect the themes and trends of Vera's long and fertile research career. We consider her career by examining her impact on the following areas of coding theory:

1. self-orthogonal and self-dual codes,
2. formally self-dual codes,
3. identities on the weight distribution,
4. covering radius,
5. families of linear codes,
6. additive codes,
7. codes and block designs,
8. codes over rings,
9. decoding, and
10. cryptography

Also within each of Sects. 1 through 10 (except Sect. 4) we include brief synopses of the articles in this issue that pertain to the topic of the section; additional papers in this issue are then listed in Sect. 11. We conclude with a description of Vera's books and then present a concluding summary and tribute to Vera Pless.

✉ Jon-Lark Kim
ctryggoggo1@gmail.com; jlkim@sogang.ac.kr

W. Cary Huffman
whuffma@luc.edu

Patrick Solé
sole@enst.fr

1 Department of Mathematics and Statistics, Loyola University, Illinois, Chicago, USA

2 Department of Mathematics, Sogang University, Seoul, Korea

3 I2M (University of Aix-Marseille, Centrale Marseille, CNRS), Marseilles, France

1 Self-orthogonal and self-dual codes

One of the most extensive areas of Vera's work was in the classification and construction of self-orthogonal and self-dual codes. Her first publication in this area, while she was at the Air Force Cambridge Research Laboratories, was the initial 1972 paper [44] that eventually attracted a number of researchers to classify self-dual codes in general. In this paper, she enumerated all $[n, \frac{n}{2}]$ binary self-dual codes of even length $2 \leq n \leq 20$ and all maximal $[n, \frac{n-1}{2}]$ binary self-orthogonal codes of odd length $3 \leq n \leq 19$. The binary self-dual codes of lengths $n = 22$ and 24 were classified by Vera and N. J. A. Sloane three years later [56]. The classification at length $n = 24$ relied on Vera's proof of the uniqueness of the binary [24, 12, 8] Golay code [42]. Vera and her co-authors developed techniques called *gluing* and finding *children*, hinted at in her previous work, to classify binary self-dual codes of lengths $n = 26, 28, 30$ and binary self-dual doubly-even codes of length $n = 32$; see [14, 17, 46]. The classification and enumeration of all binary self-dual codes has now been completed through length $n = 40$; see [5] for a summary.

There is a long-standing open question [65] regarding the existence or non-existence of a binary self-dual [72, 36, 16] code. One approach to attempting to construct such a code is to assume the code has a particular automorphism of prime order. In [15] Vera and J. H. Conway proved that the only possible prime automorphism orders for which the code could exist are 2, 3, 5, 7, 11, 17, and 23; Vera eliminated 23 in [47] and with J. G. Thompson eliminated 17 in [57]. If such a code exists, from the work of many authors, its automorphism group has order at most 5; see, e.g., [5, Theorem 4.3.12].

In addition to binary self-dual codes, Vera was involved in the classification of self-dual codes over $\mathbb{F}_3$. These codes must have length a multiple of 4. In [39], Vera, Mallows, and Sloane classified these codes for lengths $n = 4, 8, 12$; the length $n = 12$ relied on the uniqueness of the ternary [12, 6, 6] Golay code as proved by Vera in [42]. The ternary self-dual codes in the case $n = 16$ were handled by Vera, Conway, and Sloane in [16]; the classification for $n = 20$ appeared in [59] by Vera, Sloane, and Ward. In [35], Vera, Leon, and Sloane found that there are exactly two *extremal* ternary [24, 12, 9] codes; these codes are an extended quadratic residue code and a *Pless symmetry code*. The ternary Pless symmetry codes, discovered by Vera in [43], are self-dual codes that, at least for relatively small length, have good distance properties.

Vera examined self-dual codes over $\mathbb{F}_4$. In joint work with Conway and Sloane in [16], she classified such codes that are Hermitian self-dual over $\mathbb{F}_4$ at length 16. While not a classification question, Vera, along with Gaborit, Solé, and Atkin in [25] define *Type II* Euclidean self-dual codes over $\mathbb{F}_4$ and an appropriate Gray map from $\mathbb{F}_4^n$ onto $\mathbb{F}_2^n \times \mathbb{F}_2^n$. Under this map, a Euclidean self-dual code over $\mathbb{F}_4$ is Type II precisely if its Gray image is a binary doubly-even self-dual code. Among these Type II codes over $\mathbb{F}_4$ are a subset of extended Q-codes; Q-codes are codes over $\mathbb{F}_4$ of odd length that generalize quadratic residue codes and were constructed by Vera in [49].

Vera was also involved in the classification of self-dual codes over larger fields. Interest in self-dual codes over such fields is enhanced by the fact that they contain families of codes that satisfy a modified Varshamov–Gilbert Bound that is asymptotically the same as the usual Varshamov–Gilbert Bound; this was proved by Vera and Pierce in [53]. Over $\mathbb{F}_5$, with Leon and Sloane, Vera enumerated the self-dual codes of even length n with $2 \leq n \leq 12$ and the maximal self-orthogonal codes of odd length n with $1 \leq n \leq 11$ in [36]. Over $\mathbb{F}_7$, with. Tonchev as co-author, Vera classified all self-dual and maximal self-orthogonal codes of length n with $3 \leq n \leq 9$ in [58].

One of the requirements to give a full classification of self-dual codes is to produce a count of the number of such codes. Such a count is called a *mass formula*. Vera computed mass formulas for self-orthogonal codes in [41] from which mass formulas for self-dual codes can be determined. The classification efforts required extensive computer computations. Vera developed a computer algebra package called CAMAC (Combinatorial and Algebraic Machine Aided Computation) [45] that she used in many of the classifications she performed.

For this special issue, motivated by Vera's construction of the ternary self-dual Pless symmetry codes, Choi and Kim, in **An improved upper bound on self-dual codes over finite fields GF(11), GF(19), and GF(23)**, construct so-called symmetric self-dual codes over GF(q) for $q \in \{11, 19, 23\}$ with minimum weights that exceed those of previously known self-dual codes.

In **Galois self-orthogonal constacyclic codes over finite fields** by Fu and Liu, necessary and sufficient conditions for constacyclic codes to be ℓ-Galois self-orthogonal and ℓ-Galois self-dual are presented; mass formulas for both ℓ-Galois self-orthogonal and ℓ-Galois self-dual codes are given.

2 Formally self-dual codes

A binary linear code $\mathcal{C}$ is called *formally self-dual* provided $\mathcal{C}$ and its Euclidean dual $\mathcal{C}$ have the same weight distribution. Clearly formally self-dual codes have even length and include self-dual codes; if all codewords have even weight (a requirement if the code is actually self-dual), then the code is *even*. The largest possible minimum distance d of an $[n, \frac{n}{2}]$ even formally self-dual code satisfies $d = 2\lfloor \frac{n}{8} \rfloor + 2$. Formally self-dual codes meeting this bound are called *extremal*. Vera and Kennedy classified all extremal even formally self-dual codes with $2 \le n \le 10$ in [31]. Bachoc [2] found all extremal even formally self-dual codes of length $n = 12$, and Vera, Fields, Gaborit, and Huffman found all extremal even formally self-dual codes of length $n = 14$ in [22]. No [16, 8, 6] binary code exists by [27]. There is a unique [18, 9, 6] code [64] and that code is not formally self-dual. Vera, Fields, Gaborit, and Huffman continued the classification finding all extremal even formally self-dual codes of length $n = 20$ in [23], and found over 1000 such codes at length $n = 22$.

Vera and Kim [34] examined the relationship, in an even formally self-dual code, between the number of codewords whose weights are divisible by 4 and the number that are not. If the code has length n, they also examined when the code has minimum distance $d = \lfloor \frac{n}{8} \rfloor + 2$ (the code is *extremal*) and when the code has minimum distance $d = \lfloor \frac{n}{8} \rfloor$ (the code is *near-extremal*).

In Vera's paper on even formally self-dual codes [22], part of the construction relied on an examination of the hull of a code, the intersection of a code and its dual. Self-dual codes have hulls as large as possible. Codes with minimal size hulls are at the opposite end; this special issue contains two papers dealing with small hulls. If the hull is trivial, the code in called LCD; LCD codes are used in protection against side channel attacks in cryptography. In **A new method for constructing linear codes with small hulls**, the authors Qian, Cao, Lu, and Solé develop construction methods for LCD codes and codes with hulls of dimension 1. Sok, in **A new construction of linear codes with one-dimensional hull**, constructs codes with one-dimensional hulls and gives applications to quantum error-correction.

3 Identities on the weight distribution

In her 1962 Ph.D. thesis [38], MacWilliams gave a sequence of equations involving binomial coefficients relating the weight distribution of a linear code $\mathcal{C}$ and that of its Euclidean dual $\mathcal{C}^\perp$. From these equations, the number of codewords in $\mathcal{C}^\perp$ of a given weight can be determined from the total weight distribution of $\mathcal{C}$ via Krawtchouck polynomials. The relationship is often given as a single polynomial equation relating the weight enumerators of the two codes. A year later Vera Pless in [40] gave sequences of equations involving binomial coefficients and Stirling numbers relating the weight distributions of $\mathcal{C}$ and $\mathcal{C}^\perp$. This formulation has become known as the *Pless Power Moments*. The equivalence of the Pless Power Moments and the MacWilliams Equations is proved in [30, Theorem 2.3]. For a given situation, one formulation may be preferred over the other.

When the code is self-dual, these equations can be used to give specific weight distributions of the code and information about its minimum weight. They are important in the classification and enumeration of self-dual and formally self-dual codes. They also give information about the possibility of codewords of a given weight supporting designs.

Throughout coding theory literature there are generalizations of these identities in a variety of contexts. In **Variants of Jacobi polynomials in coding theory**, Chakraborty and Miezaki introduce the complete joint Jacobi polynomial of two linear codes over $\mathbb{F}_q$ and $\mathbb{Z}_k$; among other results on these and related polynomials, they give a MacWilliams type identity for the complete joint Jacobi polynomials of codes.

4 Covering radius

Vera wrote a series of papers on the covering radius of a code. In fact, the chapter on covering radius for the *Handbook of Coding Theory* [13] was co-authored by Vera, Brualdi, and Litsyn. Her first result [1], joint with Assmus, Jr., presented bounds on the covering radius of all extremal doubly-even binary self-dual codes of length $8 \leq n \leq 96$; e.g., every doubly-even [32, 16, 8] code has covering radius 6. In a paper by Vera, Brualdi and Wilson [11], the function $l(m, r)$ is defined as the smallest length of a binary code of codimension m and covering radius r; the authors give exact values or a range of values for $l(m, r)$ with $1 \leq m \leq 12$ and $1 \leq r \leq 12$. Some of the results of this paper were improved in [6] co-authored by Vera and Brualdi. In a pair of papers published in 1990, also written with Brualdi, Vera examined the relationship between a binary code and a subcode of the code [9]; they considered [7] a chain of subcodes of a binary Hamming code and examined the covering radii of the codes in the chain.

An *orphan* is a maximal coset of a code (under a certain partial ordering); each coset whose weight equals the covering radius is an orphan but an orphan can have weight smaller than the covering radius. In two papers, the first with Brualdi [8] and the second with Brualdi and Cai [12], Vera examine the orphan structure of first order Reed–Muller codes.

5 Families of linear codes

As already alluded to, Vera discovered many families of codes; some were generalizations of other known families.

- *Symmetry Codes* [43]: These codes are defined over $\mathbb{F}_3$ and are constructed using quadratic residues and non-residues, reminiscent of quadratic residue codes. From the generator matrices, one can construct Hadamard matrices. If q is a prime power with $q \equiv 2 \pmod 3$, the symmetry code $\mathcal{S}_q$ is a $[2q + 2, q + 1]$ self-dual code. $\mathcal{S}_5$ is the [12, 6, 6] extended ternary Golay code; $\mathcal{S}_{11}$ is a [24, 12, 9] extremal self-dual code not equivalent to the only other extremal self-dual code of length 24 (an extended quadratic residue code); and $\mathcal{S}_{17}$, $\mathcal{S}_{23}$, and $\mathcal{S}_{29}$ are all extremal self-dual codes with parameters [36, 18, 12], [48, 24, 15], and [60, 30, 18], respectively. The automorphism group of $\mathcal{S}_q$ is large, containing an appropriate projective linear group.
- *Duadic Codes* [37]: The original paper, by Vera, Leon, and Masley [37], defined binary duadic codes. They were later generalized to codes over other fields. In [49], Vera extended the notion of binary duadic codes to codes over $\mathbb{F}_4$, where she called them *Q-codes*. Properties and further generalizations by Vera and others can be found in [19, 50, 60, 63, 66]. Duadic codes are generalizations of quadratic residue codes and share many of the same properties; see, e.g., [30, Chapter 6]. They are cyclic codes defined in two pairs by related idempotents, a pair of even-like codes and a pair of odd-like codes.
- *Triadic Codes* [55]: Triadic codes are cyclic codes defined in two triples by related idempotents, a triple of even-like codes and a triple of odd-like codes.
- *Greedy Codes* [10]: These binary linear codes, discovered by Vera and Brualdi, are generalizations of lexicodes. To construct a greedy code, fix an ordering of $\mathbb{F}_2^n$ and a positive integer d. Apply a specified greedy algorithm to construct the code. The result is a binary linear code of length n and minimum distance at least d.

For this special issue, in **On Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs**, Tonchev proves that a specific code which is monomially equivalent to the Pless symmetry code of length $2q + 2$ contains the (0, 1)-incidence matrix of a Hadamard 3-$(2q + 2, q + 1, (q - 1)/2)$ design associated with a Paley–Hadamard matrix of type II; a similar connection exists between an extended quadratic residue code and a Hadamard 3-design associated with a Paley-Hadamard matrix of type I. All Hadamard matrices of order 36 formed by codewords of the Pless symmetry code of length 36 are enumerated and classified up to equivalence.

6 Additive codes

Vera's work generally examined linear codes over fields. But she did venture into the study of additive codes over $\mathbb{F}_4$. In [24], with Gaborit, Huffman, and Kim, she examined the classification of Type I and Type II Hermitian trace self-dual additive codes over $\mathbb{F}_4$ of length n with $8 \leq n \leq 16$. Such codes of length $1 \leq n \leq 7$ and those of Type II at length $n = 8$ were previously classified. They completely classified the Type I codes of length 8, all the codes of lengths 9 and 11, and the Type II codes of length 12. They found lower bounds on the number of codes for the remaining lengths. (Since this paper was published, the classification has been extended completely through length 12; see [18].)

Additive codes have assumed an important place in coding literature. In this issue there is one article on additive codes over the mixed alphabet $\mathbb{Z}_p\mathbb{Z}_{p^2}$. Wu and Shi, in **On $\mathbb{Z}_2\mathbb{Z}_4$-additive polycyclic codes and their Gray images**, construct generator polynomials and minimal generating sets for polycyclic codes over $\mathbb{Z}_2\mathbb{Z}_4$. In particular, under a specific inner product, the authors study the dual of $\mathbb{Z}_2\mathbb{Z}_4$-additive polycyclic codes.

7 Codes and block designs

The Assmus–Mattson Theorem gives conditions on the parameters of a linear code over a field that guarantees when codewords of a fixed weight hold a t-design. Some of the papers mentioned above, written by Vera and her coauthors, presented codes with codewords holding designs. Additionally, in [33], Vera and Kim proved a version of the Assmus–Mattson Theorem that applied to additive codes over $\mathbb{F}_4$.

In **Quadratic residue codes, rank three groups and PBIBDs** by Shi, Wang, Helleseth, and Solé, the authors study the Zetterberg code and related codes which have rank three automorphism groups; the presence of these rank three groups shows that the codes have codewords of certain weights that support partial balanced incomplete block designs.

In **Symmetric functions and spherical t-designs in** $\mathbb{R}^2$, Martínez constructs spherical t-designs on the unit sphere in $\mathbb{R}^2$; the author defines the concept of k elements being in *t-good position* on the unit sphere and then shows that $2t$ unit sphere points can be added to k of these t-good elements to form a spherical t-design with $2t + k$ points.

In **Moderate-density parity-check codes from projective bundles**, Bariffi, Mattheus, Neri, and Rosenthal propose new constructions for moderate-density parity-check codes using finite geometry. In particular, they construct a parity-check matrix for a family of these binary codes as the concatenation of two matrices: the incidence matrix between points and lines of the Desarguesian projective plane and the incidence matrix between points and ovals of a projective bundle.

8 Codes over rings

While certainly the bulk of Vera's work dealt with codes over fields, she did publish a few papers on codes over the ring $\mathbb{Z}_4$. In [54], with her student Qian, she presented a pair of generators of a $\mathbb{Z}_4$-linear cyclic code $\mathcal{C}$ of odd length n in terms of three polynomials whose product is $x^n - 1$. From this the generators of the dual cyclic code can be determined. They also presented analogues of quadratic residue codes over $\mathbb{Z}_4$. In [62], Vera, Qian, and Solé, determined when $\mathbb{Z}_4$-linear cyclic codes are self-dual. Returning to her roots in classification, Vera along with Fields, Gaborit, and Leon, classified and enumerated [21] all $\mathbb{Z}_4$-linear self-dual codes of length n with $10 \leq n \leq 15$ (the cases $1 \leq n \leq 9$ were already known). Vera, Fields, and Leon extended the classification to length 16, but only the codes of Type II, in [61].

Not only was Vera interested in cyclic codes over $\mathbb{Z}_4$, but her interests extended to cyclic codes over fields and finding idempotent generators (e.g., in duadic and triadic codes). Finding idempotent generators of skew-cyclic codes is one of the topics of (θ, δ_θ)**-cyclic codes over** $\mathbb{F}_q[u, v]/\langle u^2 - u, v^2 - v, uv - vu\rangle$ by S. Patel and O. Prakash published in this special issue.

Alahmadi, Alkathiry, Altassan, Bonnecaze, Shoaib, and Solé in **The build-up construction over a commutative non-unital ring** study construction methods for quasi self-dual codes over a commutative ring of order 4 without identity; the authors classify these codes for certain lengths and connect them to additive codes over $\mathbb{F}_4$.

Codes over Galois rings play a significant role in the study of codes over rings. In **Weight distribution of double cyclic codes over Galois rings** by Gao, Meng, and Fu, the authors determine the weight distribution of several classes of double cyclic codes over Galois rings by using Gauss sums.

When examining codes over rings, one problem is to consider when two codes are equivalent. One property that maps defining equivalence should possess is that they preserve weights. MacWilliams [38] proved essentially that a Hamming weight preserving linear transformation between two linear codes over a field extends to a monomial map on the ambient space. This so-called MacWilliams Extension Theorem is the subject of **MacWilliams extension property for arbitrary weights on linear codes over module alphabets** by Dyshko and Woods in the case where the alphabet is a finite pseudo-injective module with a cyclic socle equipped with an arbitrary weight.

9 Decoding

Vera did limited work on decoding algorithms with her papers dedicated to decoding certain codes by hand. In [48], she described decoding the [24, 12, 8] extended binary Golay code and the [12, 6, 6] extended ternary Golay code. The process was to project received vectors onto the hexacode, a [6, 3, 4] Hermitian self-dual code over $\mathbb{F}_4$, or onto the tetracode, a self-dual [4, 2, 3] ternary code, respectively. With knowledge of the structure of these projected codes, one can decode received vectors by hand by following a prescribed algorithm that she developed. Several years later, first with Kim [32] and then with Gaborit and Kim [26], using analogous projection techniques, she was able to decode the [32, 16, 8] self-dual Reed–Muller code and other [32, 16, 8] self-dual codes also by hand.

There are several classes of codes whose development was designed to make decoding efficient for the given setting. Three papers appear in this special issue that investigate decoding properties and algorithms for various families of codes.

The article **Decoding algorithms of monotone codes and azinv codes and their unified view**, by Takahashi and Hagiwara, investigates linear-time decoding algorithms for two classes of error-correcting codes: monotone codes and azinv codes. Also, the authors propose generalizations of Levenshtein's decoding algorithm for single deletion or single substitution error-correcting codes.

Subspace codes can be used for error control in random linear network coding. In **Parallel sub-code construction for constant-dimension codes**, He, Chen, Zhang, and Zhou show how to improve the construction of subspace codes from two parallel versions of the sub-code construction, allowing them to find larger constant-dimension code sizes.

Layered codes are used for distributed storage systems. In **Johnson graph codes**, Duursma and Li show that the concatenation of layered codes with suitable outer codes achieves the performance of other known codes that are conjectured to be optimal for general regenerating codes. The outer codes used are in a new class of codes called Johnson graph codes, which have properties similar to those of Reed–Muller codes.

10 Cryptography

With Beissinger, Vera wrote a book [3] explaining the basics of cryptography and how cryptography relates to coding theory. This book, *The Cryptoclub: Using Mathematics to Make and Break Secret Codes*, introduces elementary and middle school students to the world of secret codes and how mathematics plays a role in the making and breaking of secret messages.

In this special issue there are two articles applying coding theory to cryptography. In **A gapless code-based hash proof system based on RQC and its applications** by Bettaieb, Bidoux, Blazy, Connan, and Gaborit, the authors show how to build a hash proof system from code-based cryptography and present a way, based on a proof of knowledge, to fully negate a problematic gap to protect against an undetectable attack. The authors Ayebie and Souidi of **New code-based cryptographic accumulator and fully dynamic group signature** propose a code-based cryptographic accumulator that is quantum computer resistant. This scheme is based on the hardness of the Syndrome Decoding Problem; it also uses double circulant codes allowing for small key sizes.

11 Other articles in this issue

Vera always encouraged her students and colleagues to continue to pursue their research interests in a variety of areas of coding theory. A few articles appear in this issue on topics that have not been listed above.

Character sums appear in several places in coding literature. In **Further improvement on index bounds** by Wu, Lee, and Wang, the authors obtain examples which show improvement of both the index bound of Wan and Wang and the Weil bound for character sums; using their results, they give an estimation of the number of solutions of some algebraic curves. A new application of the Weil bound for character sums is used to give some direct constructions of pairwise 2-compatible balanced difference families in **Compatible difference packing set systems and their applications to multilength variable-weight OOCs** by Qin, Zhao, and Yu. Additionally, some series of compatible difference packing set systems are produced yielding several infinite classes of optimal multilength variable-weight optical orthogonal codes.

Steganography is the science of communicating a secret message by hiding it in a cover object. In **Steganography from perfect codes on Cayley graphs over Gaussian integers, Eisenstein-Jacobi integers and Lipschitz integers**, Kim and Park construct steganographic schemes explicitly from r-perfect codes on Cayley graphs over Gaussian, Eisenstein-Jacobi, and Lipschitz integers.

In **The concatenated structure of quasi-abelian codes**, Borello, Güneri, Saçıkara, and Solé give a concatenated decomposition of quasi-abelian codes allowing them to present a general minimum distance bound for quasi-abelian codes and to construct some optimal codes; they conclude that strictly quasi-abelian linear complementary dual codes over any finite field are asymptotically good.

The authors Jafari, Abdollahi, Bagherian, Khatami, and Sobhani of **Equidistant permutation group codes** study subgroups of the symmetric group on $\{1, 2, \ldots, n\}$ all of whose non-trivial permutations have a constant number of fixed points; in particular they present a type of classification theorem for such codes.

In **Classification of weighted posets and digraphs admitting the extended Hamming code to be a perfect code** by Kim and Kwon, the authors consider metrics arising from digraphs and from weighted posets. For certain parameters, they classify all structure vectors of digraphs and of weighted posets which admit the extended Hamming code to be a 2-perfect code.

In **Construction of asymmetric Chudnovsky-type algorithms for multiplication in finite fields** by Ballet, Baudru, Bonnecaze, and Tukumuli, the authors study an algorithm by Chudnovsky and Chudnovsky for the multiplication in extensions of finite fields generalized by Randriambololona. They propose a generic strategy to construct these algorithms using concepts from algebraic geometry.

12 Vera's books

In addition to the cryptography book [3], Vera Pless wrote or edited three books on error-correcting codes. Her first coding theory book, *Introduction to the Theory of Error-Correcting Codes*, appeared in 1982. The current edition, the 3rd, was published in 1998 [51]. Vera and Huffman edited the 25 chapter two volume *Handbook of Coding Theory* [52] written by 33 authors, which also appeared in 1998; this work led the reader to the frontiers of research. In 2003, they co-authored *Fundamentals of Error-Correcting Codes* that was intended to be a bridge to the *Handbook*.

13 Summary

As editors of this special issue dedicated to Vera Pless, we trust that the articles reflect her research interests. Her contribution to the study of error-correcting codes is certainly very long-lasting. One of us (Jon-Lark Kim) was a Ph.D. student of Vera and a co-author over several years. Cary Huffman and Patrick Solé were colleagues and co-authors greatly influenced by her work. We would like to end with a quote from the final paragraph in Huffman's memorial tribute to Vera [28]:

> On a personal note, I had the privilege of working with Vera for over 30 years as our universities were only a subway ride (with one transfer) apart. Vera was always inspirational with her wealth of knowledge and intuitive insight into coding problems. In a very informal way, she taught me much coding theory as we sat in her office, probably not realizing how influential these conversations were. Vera loved classical music and reading; she loved her children and grandchildren. And she loved her students. On my visits, we would often go to lunch, usually at Vera's favorite Thai restaurant, inviting one or two students; you could never move fast enough as she would quickly pick up the check. I served on the Ph.D. committees of a number of her students. When members would ask the student a question, Vera could barely restrain herself (and often did not) from answering for them—she so much wanted her students to succeed. In the days following her passing, I received emails from coding theorists whose research careers were nudged, and even re-directed, along new paths based on interactions with Vera. Her presence will be greatly missed.

References

1. Assmus E.F. Jr., Pless V.S.: On the covering radius of extremal self-dual codes. IEEE Trans. Inform. Theory **29**, 359–363 (1983).
2. Bachoc C.: On harmonic weight enumerators of binary codes. Des. Codes Cryptogr. **18**, 11–28 (1999) **Designs and codes—a memorial tribute to Ed Assmus**.
3. Beissinger J., Pless V.S.: The Cryptoclub: Using Mathematics to Make and Break Secret Codes. CRC Press, Boca Raton (2006).
4. Biographies of Women Mathematicians. https://mathwomen.agnesscott.org/women/pless.htm.
5. Bouyuklieva S.: Self-dual codes. In: Huffman W.C., Kim J.-L., Solé P. (eds.) Concise Encyclopedia of Coding Theory, Chapter 4, pp. 79–96. CRC Press, Boca Raton (2021).

6. Brualdi R.A., Pless V.S.: On the length of codes with a given covering radius. In: Coding Theory and Design Theory, Part I, volume 20 of IMA Vol. Math. Appl., pp. 9–15. Springer, New York (1990).
7. Brualdi R.A., Pless V.S.: Subcodes of Hamming codes. In Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989), vol. 70, pp. 153–158 (1990).
8. Brualdi R.A., Pless V.S.: Orphans of the first order Reed–Muller codes. IEEE Trans. Inform. Theory **36**, 399–401 (1990).
9. Brualdi R.A., Pless V.S.: On the covering radius of a code and its subcodes. Discret. Math. **83**, 189–199 (1990).
10. Brualdi R.A., Pless V.S.: Greedy codes. J. Comb. Theory Ser. A **64**, 10–30 (1993).
11. Brualdi R.A., Pless V.S., Wilson R.M.: Short codes with a given covering radius. IEEE Trans. Inform. Theory **35**, 99–109 (1989).
12. Brualdi R.A., Cai N., Pless V.S.: Orphan structure of the first order Reed–Muller codes. Discret. Math. **102**, 239–247 (1992).
13. Brualdi R.A., Litsyn S., Pless V.S.: Covering Radius. In: Pless V.S., Huffman W.C. (eds.) Handbook of Coding Theory, Vol. I, II, Chapter 8, pp. 755–826. North-Holland, Amsterdam (1998).
14. Conway J.H., Pless V.S.: On the enumeration of self-dual codes. J. Comb. Theory Ser. A **28**, 26–53 (1980).
15. Conway J.H., Pless V.S.: On primes dividing the group order of a doubly-even (72, 36, 16) code and the group order of a quaternary (24, 12, 10) code. Discret. Math. **38**, 143–156 (1982).
16. Conway J.H., Pless V.S., Sloane N.J.A.: Self-dual codes over GF(3) and GF(4) of length not exceeding 16. IEEE Trans. Inform. Theory **25**, 312–322 (1979).
17. Conway J.H., Pless V.S., Sloane N.J.A.: The binary self-dual codes of length up to 32: a revised enumeration. J. Comb. Theory Ser. A **60**, 183–195 (1992).
18. Danielsen L.E.: Database of self-dual quantum codes. http://www.ii.uib.no/~larsed/vncorbits.
19. Ding C., Pless V.S.: Cyclotomy and duadic codes of prime lengths. IEEE Trans. Inform. Theory **45**, 453–466 (1999).
20. Dougherty S.T., Matthews G., Wood J.: The life and work of Vera Stepen Pless. (2022).
21. Fields J.E., Gaborit P., Leon J.S., Pless V.S.: All self-dual $\mathbb{Z}_4$ codes of length 15 or less are known. IEEE Trans. Inform. Theory **44**, 311–322 (1998).
22. Fields J.E., Gaborit P., Huffman W.C., Pless V.S.: On the classification of extremal even formally self-dual codes. Des. Codes Cryptogr. **18**, 125–148 (1999).
23. Fields J.E., Gaborit P., Huffman W.C., Pless V.S.: On the classification of extremal even formally self-dual codes of lengths 20 and 22. Discret. Appl. Math. **111**, 75–86 (2001).
24. Gaborit P., Huffman W.C., Kim J.-L., Pless V.S.: On additive GF(4) codes. In Codes and Association Schemes (Piscataway, NJ, 1999), volume 56 of DIMACS Ser. Discret. Math. Theoret. Comput. Sci. pp. 135–149. Amer. Math. Soc., Providence, RI (2001)
25. Gaborit P., Pless V.S., Solé P., Atkin O.: Type II codes over $\mathbb{F}_4$. Finite Fields Appl. **8**, 171–183 (2002).
26. Gaborit P., Kim J.-L., Pless V.S.: Decoding binary $R(2, 5)$ by hand. Discret. Math. **264**, 55–73 (2003).
27. Grassl M.: Code tables: Bounds on the parameters of various types of codes. http://www.codetables.de.
28. Huffman W.C.: A tribute to Vera Pless (1931–2020). Finite Fields Appl. **65**, 101675 (2020).
29. Huffman W.C.: In Memorium: Vera Stepen Pless. https://www.itsoc.org/news-events/recent-news/in-memoriam-vera-stepen-pless.
30. Huffman W.C., Pless V.S.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
31. Kennedy G., Pless V.S.: On designs and formally self-dual codes. Des. Codes Cryptogr. **4**, 43–55 (1994).
32. Kim J.-L., Pless V.S.: Decoding some doubly-even self-dual [32, 16, 8] codes by hand. In: Codes and Designs (Columbus, OH, 2000), vol. 10 of Ohio State Univ. Math. Res. Inst. Publ., pp. 165–178. de Gruyter, Berlin (2002)
33. Kim J.-L., Pless V.S.: Designs in additive codes over GF(4). Des. Codes Cryptogr. **30**, 187–199 (2003).
34. Kim J.-L., Pless V.S.: A note on formally self-dual even codes of length divisible by 8. Finite Fields Appl. **13**, 224–229 (2007).
35. Leon J.S., Pless V.S., Sloane N.J.A.: On ternary self-dual codes of length 24. IEEE Trans. Inform. Theory **27**, 176–180 (1981).
36. Leon J.S., Pless V.S., Sloane N.J.A.: Self-dual codes over GF(5). J. Comb. Theory Ser. A **32**, 178–194 (1982).
37. Leon J.S., Masley J.M., Pless V.S.: Duadic codes. IEEE Trans. Inform. Theory **30**, 709–714 (1984).
38. MacWilliams F.J.: Combinatorial Problems of Elementary Abelian Groups. PhD thesis, Harvard University (1962)
39. Mallows C.L., Pless V.S., Sloane N.J.A.: Self-dual codes over GF(3). SIAM J. Appl. Math. **31**, 649–666 (1976).

40. Pless V.S.: Power moment identities on weight distributions in error correcting codes. Inform. Control **6**, 147–152 (1963).
41. Pless V. S.: The number of isotropic subspaces in a finite geometry. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8) **39**, 418–421 (1965).
42. Pless V.S.: On the uniqueness of the Golay codes. J. Comb. Theory **5**, 215–228 (1968).
43. Pless V.S.: On a family of symmetry codes over GF(3) and related new five-designs. In Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969), pp. 323–326. Gordon and Breach, New York (1970).
44. Pless V.S.: A classification of self-orthogonal codes over GF(2). Discret. Math. **3**, 209–246 (1972).
45. Pless V.S.: CAMAC—Combinatorial and Algebraic Machine Aided Computation. In Proc. of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Florida Atlantic Univ., Boca Raton, FL, 1975), pp. 505–511. Congressus Numerantium, No,. XIV, (1975)
46. Pless V.S.: The children of the (32, 16) doubly even codes. IEEE Trans. Inform. Theory **24**, 738–746 (1978).
47. Pless V.S.: 23 does not divide the order of the group of a (72, 36, 16) doubly even code. IEEE Trans. Inform. Theory **28**, 113–117 (1982).
48. Pless V.S.: Decoding the Golay codes. IEEE Trans. Inform. Theory **32**, 561–567 (1986).
49. Pless V.S.: Q-codes. J. Comb. Theory Ser. A **43**, 258–276 (1986).
50. Pless V.S.: Duadic codes and generalizations. In: Camion P., Charpin P., Harari S. (eds.) Proc. International Symposium on Information Theory – EUROCODE 1992, volume 339 of CISM Courses and Lect., pages 3–15. Springer, Vienna (1993)
51. Pless V.S.: Introduction to the Theory of Error-Correcting Codes, 3rd edn Wiley, New York (1998).
52. Pless V.S., Huffman W.C. (eds.): Handbook of Coding Theory. II, vol. I. North-Holland, Amsterdam (1998).
53. Pless V.S., Pierce J.N.: Self-dual codes over GF(q) satisfy a modified Varshamov–Gilbert bound. Inf. Control **23**, 35–40 (1973).
54. Pless V.S., Qian Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory **42**, 1594–1600 (1996).
55. Pless V.S., Rushanan J.J.: Triadic codes. Linear Algebra Appl. **98**, 415–433 (1988).
56. Pless V.S., Sloane N.J.A.: On the classification and enumeration of self-dual codes. J. Comb. Theory Ser. A **18**, 313–335 (1975).
57. Pless V.S., Thompson J.G.: 17 does not divide the order of the group of a (72, 36, 16) doubly even code. IEEE Trans. Inform. Theory **28**, 537–541 (1982).
58. Pless V.S., Tonchev V.D.: Self-dual codes over GF(7). IEEE Trans. Inform. Theory **33**, 723–727 (1987).
59. Pless V.S., Sloane N.J.A., Ward H.N.: Ternary codes of minimum weight 6 and the classification of the self-dual codes of length 20. IEEE Trans. Inform. Theory **26**, 305–316 (1980).
60. Pless V.S., Masley J.M., Leon J.S.: On weights in duadic codes. J. Comb. Theory Ser. A **44**, 6–21 (1987).
61. Pless V.S., Leon J.S., Fields J.E.: All $\mathbb{Z}_4$ codes of type II and length 16 are known. J. Comb. Theory Ser. A **78**, 32–50 (1997).
62. Pless V.S., Solé P., Qian Z.: Cyclic self-dual $\mathbb{Z}_4$-codes. Finite Fields Appl. **3**, 48–69 (1997).
63. Rushanan J.J.: Generalized Q-Codes. PhD thesis, California Institute of Technology (1986)
64. Simonis J.: The [18, 9, 6] code is unique. Discret. Math. **106**(107), 439–448 (1992).
65. Sloane N.J.A.: Is there a (72, 36) $d = 16$ self-dual code? IEEE Trans. Inform. Theory **19**, 251 (1973).
66. Smid M.H.M.: Duadic codes. IEEE Trans. Inform. Theory **33**, 432–433 (1987).
67. Vera Pless. https://mathshistory.st-andrews.ac.uk/Biographies/Pless/.