The Perfect Binary One-Error-Correcting Codes of Length 15: Part II—Properties

Patric R. J. Östergård, Olli Pottonen, Kevin T. Phelps

Abstract—A complete classification of the perfect binary one-error-correcting codes of length 15 as well as their extensions of length 16 was recently carried out in [P. R. J. Östergård and O. Pottonen, “The perfect binary one-error-correcting codes of length 15: Part I—Classification,” IEEE Trans. Inform. Theory vol. 55, pp. 4657–4660, 2009]. In the current accompanying work, the classified codes are studied in great detail, and their main properties are tabulated. The results include the fact that 33 of the 80 Steiner triple systems of order 15 occur in such codes. Further understanding is gained on full-rank codes via switching, as it turns out that all but two full-rank codes can be obtained through a series of such transformations from the Hamming code. Other topics studied include (non)systematic codes, embedded one-error-correcting codes, and defining sets of codes. A classification of certain mixed perfect codes is also obtained.

Index Terms—classification, Hamming code, perfect code, Steiner system, switching

I. INTRODUCTION

We consider binary codes of length $n$ over the Galois field $\mathbb{F}_2$, that is, subsets $C \subseteq \mathbb{F}_2^n$. The (Hamming) distance $d(x,y)$ between two words $x$, $y$ is the number of coordinates in which they differ, and the (Hamming) weight $w_t(x)$ of a word $x$ is the number of nonzero coordinates. The support of a word is the set of nonzero coordinates, that is, $\text{supp}(x) = \{i : x_i \neq 0\}$. Accordingly, $d(x,y) = w_t(x-y) = |\text{supp}(x-y)|$.

The minimum distance of a code is the largest integer $d$ such that the distance between any distinct codewords is at least $d$. The balls of radius $[(d-1)/2]$ centered around the codewords of a code with minimum distance $d$ are nonintersecting, so such a code is said to be a $[(d-1)/2]$-error-correcting code. If these balls simultaneously pack and cover the ambient space, then the code is called perfect. A t-error-correcting perfect code is also called a t-perfect code.

It is well known [11] that binary perfect codes exist exactly for $d = 1$; $d = n$; $d = (n-1)/2$ for odd $n$; $d = 3$, $n = 2^m-1$ for $m \geq 2$; and $d = 7$, $n = 23$. The first three types of codes are called trivial, the fourth has the parameters of Hamming codes, and the last one is the binary Golay code.

The number of binary 1-perfect codes of length 15 was recently determined in [2] (where the codes are also made available in electronic form) using a constructive approach. It turned out that there are 5983 inequivalent such codes, and these have 2165 inequivalent extensions. Two binary codes are said to be equivalent if one can be obtained from the other by permuting coordinates and adding a constant vector. Such a mapping that produces a code from itself is an automorphism; the set of all automorphisms of a code form a group, the automorphism group.

The complete set of inequivalent codes is a valuable tool that makes it possible to study a wide variety of properties. Our aim is to answer questions stated in [3], [4] and elsewhere, and in general to gain as good understanding as possible of the properties of the binary 1-perfect codes of length 15. The graph isomorphism program nauty [5] played a central role in several of the computations.

For completeness, we give the table with the distribution of automorphism group orders from [2] in Section III, where also the distribution of kernels is tabulated (including some corrections to earlier results). The supports of the differences between a codeword in a 1-perfect code and other codewords at (minimum) distance 3 form a Steiner triple system. In Section III such occurrences of Steiner triple systems in the codes—and occurrences of Steiner quadruple systems in the extended codes—are studied, determining among other things that exactly 33 of the 80 Steiner triple systems of order 15 occur in these 1-perfect codes. Other topics addressed include the determination of the largest number of isomorphism classes of Steiner triple systems in a code.

In Section IV partial results are provided on perhaps the most intriguing issue regarding 1-perfect codes, namely that of finding constructions (explanations) for all different codes. It turns out that the binary 1-perfect codes of length 15 are partitioned into just 9 switching classes. The technique of switching is utilized also in Section V for proving general results for defining sets of 1-perfect codes. (Non)systematic 1-perfect codes are treated in Section VI and embedded one-error-correcting codes and related orthogonal arrays are considered in Section VII.

Many classes of mixed perfect codes with alphabet sizes that are powers of 2 are classified in Section VIII. The paper is concluded in Section IX which includes a list of a few interesting problems related to binary 1-perfect codes of length 15, yet unanswered.

This work was supported in part by the Graduate School in Electronics, Telecommunication and Automation, by the Nokia Foundation, and by the Academy of Finland, Grant Numbers 107493, 110196, and 130142.

P. R. J. Östergård is with the Department of Communications and Networking, Aalto University, P.O. Box 13000, 00076 Aalto, Finland (e-mail: patric.ostergard@tkk.fi).

O. Pottonen was with the Department of Communications and Networking, Helsinki University of Technology TKK, P.O. Box 3000, 02015 TKK, Finland. He is now with the Finnish Defence Forces Technical Research Centre, P.O. Box 10, 11311 Riihimäki, Finland. (e-mail: olli.pottonen@iki.fi).

K. T. Phelps is with the Department of Mathematics and Statistics, Auburn University, Auburn, AL 36849, USA (e-mail: phelpkt@auburn.edu).

Patric R. J. Östergård is with the Department of Communications and Networking, Aalto University, P.O. Box 13000, 00076 Aalto, Finland (e-mail: patric.ostergard@tkk.fi).

O. Pottonen was with the Department of Communications and Networking, Helsinki University of Technology TKK, P.O. Box 3000, 02015 TKK, Finland. He is now with the Finnish Defence Forces Technical Research Centre, P.O. Box 10, 11311 Riihimäki, Finland. (e-mail: olli.pottonen@iki.fi).

K. T. Phelps is with the Department of Mathematics and Statistics, Auburn University, Auburn, AL 36849, USA (e-mail: phelpkt@auburn.edu).
II. AUTOMORPHISM GROUPS

First, we give formal definitions of several central concepts, some of which were briefly mentioned in the Introduction. A permutation $\pi$ of the set $\{1, 2, \ldots, n\}$ acts on codewords by permuting the coordinates in the obvious manner. Pairs $(\pi, x)$ form the wreath product $S_2 \wr S_n$, which acts on codes as $(\pi, x)(C) = \pi(C + x) = \pi(C) + \pi(x)$. Two codes, $C_1$ and $C_2$, are said to be isomorphic if $C_1 = \pi(C_2)$ for some $\pi$ and equivalent if $C_1 = \pi(C_2 + x)$ for some $\pi, x$.

The automorphism group of a code $C$, $\text{Aut}(C)$, is the group of all pairs $(\pi, x)$ such that $C = \pi(C + x)$. Two important subgroups of $\text{Aut}(C)$ are the group of symmetries, 

$$\text{Sym}(C) = \{\pi : \pi(C) = C\}$$

and the kernel

$$\text{Ker}(C) = \{x : C + x = C\}.$$ 

If the code contains the all-zero word, $0$, then the elements of the kernel are codewords. The distribution of the orders of the automorphism groups of the binary 1-perfect codes of length 15 and their extensions are presented in Table I and Table II respectively.

| AUTOMORPHISM GROUPS OF CODES | \[\text{Aut}(C)\] | # | \[\text{Aut}(C)\] | # |
|-------------------------------|-----------------|---|-----------------|---|
| 8                             | 1 017           | 24 576 | 7              |
| 12                            | 3 768           | 32 768 | 8              |
| 16                            | 5 1024          | 43 008 | 4              |
| 24                            | 7 1024          | 49 152 | 10             |
| 32                            | 138 1536        | 65 536 | 5              |
| 42                            | 2 2048          | 98 304 | 1              |
| 48                            | 12 2688         | 131 072 | 1      |
| 64                            | 542 3072        | 172 032 | 1      |
| 96                            | 22 3840         | 196 608 | 5              |
| 120                           | 1 4096          | 344 064 | 2              |
| 128                           | 1 5376          | 393 216 | 2              |
| 192                           | 18 6144         | 589 824 | 1              |
| 256                           | 1319 8192       | 41 287 680 | 1   |
| 336                           | 3 12 288        | 7               |
| 384                           | 30 16 384       | 44              |

| AUTOMORPHISM GROUPS OF EXTENDED CODES | \[\text{Aut}(C)\] | # | \[\text{Aut}(C)\] | # |
|--------------------------------------|-----------------|---|-----------------|---|
| 128                                  | 11 5 376        | 1 196 608 | 6              |
| 192                                  | 5 6 144         | 23 262 144 | 3              |
| 256                                  | 105 8 192       | 174 344 064 | 1      |
| 384                                  | 9 10 752        | 2 393 216 | 3              |
| 512                                  | 377 12 288      | 22 524 288 | 2              |
| 672                                  | 2 16 384        | 103 688 128 | 1      |
| 768                                  | 19 24 576       | 12 786 432 | 2              |
| 1024                                 | 416 32 768      | 47 1572 864 | 3          |
| 1344                                 | 1 43 008        | 2 2 539 296 | 1              |
| 1536                                 | 21 49 152       | 18 2 752 512 | 1      |
| 1920                                 | 1 61 440        | 1 3 145 728 | 1              |
| 2048                                 | 394 65 536      | 33 5 505 024 | 2              |
| 2688                                 | 1 86 016        | 3 6 291 456 | 1              |
| 3072                                 | 18 98 304       | 12 660 602 880 | 1     |
| 4096                                 | 298 131 072     | 6               |

The orbits of codewords of the binary 1-perfect codes of length 15 and their extensions are tabulated in Tables III and IV respectively. Here the notation $g_1 a_1 g_2 a_2 \cdots g_m a_m$ means that the number of orbits of size $g_i$ is $a_i$.

It has been known since the early days of coding theory [6], [7] that binary 1-perfect codes are distance invariant, that is, the distance distribution of the other codewords with respect to any codeword does not depend on the choice of codeword. In particular, there is always one codeword at distance $n$, that is, the all-one word is in the kernel of all binary 1-perfect codes; the codes are said to be self-complementary. The distance distribution for binary 1-perfect codes of length 15 is

$$0 \ 1 \ 7 \ 28 \ 84 \ 189 \ 315 \ 400 \ 400 \ 315 \ 189 \ 84 \ 28 \ 7 \ 1 \ 0.$$ 

There is also only one distance distribution with respect to any word that is not a codeword of such a code:

$$0 \ 1 \ 7 \ 28 \ 84 \ 189 \ 315 \ 400 \ 400 \ 315 \ 189 \ 84 \ 28 \ 7 \ 1 \ 0.$$ 

Once the equivalence classes of codes have been classified, classifying the isomorphism classes is straightforward. Isomorphic codes necessarily belong to the same equivalence class, so representatives from the isomorphism classes can be obtained by translating representatives from the equivalence classes. The following theorem characterizes the situation further.

**Theorem 1:** The codes $C + x$ and $C + y$ are isomorphic if and only if $x$ and $y$ are in the same $\text{Aut}(C)$-orbit.

**Proof:** The codes are isomorphic iff there is a permutation $\pi$ such that $\pi(C + x) = C + y$, which is equivalent to $C = \pi(C + x + \pi^{-1}(y))$. The last equation holds iff $(\pi, x + \pi^{-1}(y)) \in \text{Aut}(C)$. Clearly this pair maps $x$ to $y$. Conversely, every pair which maps $x$ to $y$ is of the type $(\pi, x + \pi^{-1}(y))$ with $\pi$ arbitrary.

There are 1 637 690 isomorphism classes of binary 1-perfect codes of length 15, 139 350 of which contain the all-zero codeword. The groups of symmetries of these codes are tabulated in Table V. The extended 1-perfect codes have 347 549 isomorphism classes, of which 22 498, 139 350, and 185 701 contain a codeword with minimum weight 0, 1, and 2, respectively. The groups of symmetries of these codes are listed in Table VI.

**Theorem 2:** An (extended) binary 1-perfect code $C$ contains an embedded (extended) binary 1-perfect code on the coordinates that are fixed by any subgroup $G \subseteq \text{Sym}(C)$.

**Proof:** Let $C$ be a binary 1-perfect code and $T$ the set of coordinates not fixed by $G$, and let $H$ be the set of all words that have zeros for all coordinates in $T$. Now consider the embedded code $C' = C \cap H$. The code $C'$ is 1-perfect (after deleting the coordinates in $T$) if every word in $H$ is at distance at most 1 from a codeword in $C'$. Now assume that this is not the case, that is, that there is a word $x \in H$ that is at distance at least 2 from all words in $C'$.

Since $C$ is a 1-perfect code, there must be a codeword $y \in C \setminus C'$ such that $d(x, y) = 1$. Moreover, since $y \notin C'$, it follows that $|\text{supp}(y) \cap T| = 1$. As there is a $\pi \in G$ such that $\pi(y) \neq y$ and $\pi$ preserves the weight within $T$, we get that $d(y, \pi(y)) = 2$. This is a contradiction since both $y$ and $\pi(y)$ are codewords and $C$ has minimum distance 3.

To prove the claim for an extended binary 1-perfect code $C$, first puncture the code at any coordinate fixed by $G$ and use the previous result for binary 1-perfect codes; extension
of the embedded 1-perfect code thereby obtained indeed gives a subcode of $C$ (as all coordinates that are deleted have value 0 for this subcode).

Note that Theorem 2 can be generalized by instead of Sym(C) considering the subgroup of Aut(C + x) that stabilizes x for any word x. Also note that Theorem 2 implies that Sym(C) has $2^k - 1$ fixed coordinates for any binary 1-perfect code C, and 0 or $2^k$ fixed coordinates for any extended binary 1-perfect code C. The numbers of fixed coordinates are tabulated in Tables VII and VIII.

The existence problem for binary 1-perfect codes with automorphism group of (minimum) order 2 has received some attention. By Table I there are no such codes of length 15. This contradicts claims in [4] p. 242 regarding existence of such codes. Existence for admissible lengths at least $2^k - 1$ and an interval of ranks has been proved in [8]. For lengths

Table III

| Orbits | # | Orbits | # |
|--------|---|--------|---|
| 3      | 32  | 5      | 192 |
| 4      | 33  | 53     | 39 |
| 5      | 226 | 6      | 256 |
| 3     3  | 32  | 53     | 53 |
| 4      | 33  | 39     | 39 |
| 5      | 226 | 256    | 256 |

Table IV

| Orbits | # | Orbits | # |
|--------|---|--------|---|
| 2      | 32  | 12     | 256 |
| 3      | 46  | 192    | 192 |
| 4      | 50  | 256    | 256 |
| 5      | 226 | 1024   | 1024 |

Table V

| Groups of Symmetries of Codes | Sym(C) | # | Sym(C) | # | Sym(C) | # |
|-------------------------------|-------|---|-------|---|-------|---|
| [1]                           | 1     | 668929 | 12 | 80 | 96 | 37 |
| [2]                           | 2     | 646808 | 16 | 2222 | 168 | 3 |
| [3]                           | 3     | 5384 | 21 | 45 | 192 | 32 |
| [4]                           | 4     | 488221 | 24 | 536 | 288 | 1 |
| [5]                           | 5     | 32685 | 344 | 7 |
| [6]                           | 6     | 648 | 48 | 24 | 20160 | 1 |
| [7]                           | 7     | 27370 | 64 | 24 | 101 |
2^m - 1 with m = 5, 6, 7, only an 8-line outline of proof has been published [9]; there is an obvious desire for a detailed treatment of those cases.

In Table IX we display the number of codes with respect to their rank and kernel size. The results for rank 15 are new, and have arrived at results that corroborate those presented elsewhere.

As can be seen, there are 398 codes with full rank. Partial results for rank 15 can be found in [12]. All possible kernels (unique for sizes 2, 4, and 8; two for sizes 16 and 32) of the full-rank codes are, up to isomorphism, generated by the observation regarding the structure of full-rank tilings of \( F_2 \), 10 \( \leq \) i \( \leq \) 15, where one of the sets has size 16, cf. [13, 14, 3]. Nonexistence of full-rank binary 1-perfect codes of length 15 with a kernel of size 64 corroborates the result in [15] that there are no full-rank tilings of \( F_2^i \) with \( |V| = 2^i \) and \( |A| = 2^h \) at the very end of [15] now gets an independent verification.

The number of extended binary 1-perfect codes of length 16 with respect to their rank and kernel size is shown in Table XI.

The kernels for the extended binary 1-perfect codes of length 16 and rank 15 are exactly those obtained by extending the kernels for the full-rank binary 1-perfect codes of length 15, listed in Table X.

## III. Steiner Systems in 1-Perfect Codes

A Steiner system \( S(t, k, v) \) is a collection of \( k \)-subsets (called blocks) of a \( v \)-set of points, such that every \( t \)-subset of the \( v \)-set is contained in exactly one block. Steiner systems \( S(2, 3, v) \) and \( S(3, 4, v) \) are called Steiner triple systems and Steiner quadruple systems, respectively, and are often referred to as STS\( (v) \) and SQS\( (v) \), where \( v \) is called the order of the system. These are related to binary 1-perfect codes in the following way.

If \( C \) is a binary 1-perfect code of length \( v \) and \( x \in C \), then the codewords of \( C + x \) with weight 3 form a Steiner triple system of order \( v \). Analogously, if \( C \) is an extended binary 1-perfect code and \( x \in C \), then the codewords of \( C + x \) with weight 4 form a Steiner quadruple system.

There are 80 Steiner triple systems of order 15. The long-standing open question whether all Steiner triple systems of...
order $2^m - 1$ occur in some binary 1-perfect code of length $2^m - 1$ was settled in [16], by showing that at least two of the 80 STS(15) do not occur in a 1-perfect code. We are now able to determine exactly which STS(15) occur in a binary 1-perfect code—the total number of such STS(15) is 33—and furthermore in how many codes each such system occurs. This information is given in Table XII using the numbering of the STS(15) from [17]. As far as the authors are aware, existence results for all of these, except those with indices 25 and 26, can be found in the literature [18], [19], [20].

Table XII

| Index | # Index | Index | # Index |
|-------|---------|-------|---------|
| 1     | 205     | 12    | 640     |
| 2     | 1543    | 13    | 1666    | 25    | 158     |
| 3     | 1665    | 14    | 1268    | 26    | 158     |
| 4     | 3623    | 15    | 1961    | 29    | 187     |
| 5     | 2209    | 16    | 745     | 33    | 37      |
| 6     | 1229    | 17    | 781     | 35    | 2       |
| 7     | 335     | 18    | 1653    | 39    | 2       |
| 8     | 3290    | 19    | 204     | 54    | 2       |
| 9     | 2950    | 20    | 493     | 61    | 57      |
| 10    | 2014    | 21    | 50      | 64    | 29      |
| 11    | 636     | 22    | 55      | 76    | 6       |

It is not difficult to see that all Steiner triple systems in a linear code are necessarily equal, so Hamming codes show that the problem of minimizing the number of different Steiner triple systems in a binary 1-perfect code has an obvious solution (for all lengths $2^m - 1$). On the other hand, Table XIII shows that 14 is the maximum number of isomorphism classes of Steiner triple systems in a binary 1-perfect code of length 15. The distribution in Table XIII is perhaps more even than one might have guessed.

Table XIII

| Size # | Size # | Size # |
|--------|--------|--------|
| 1      | 101    | 11     |
| 2      | 97     | 12     |
| 3      | 77     | 13     |
| 4      | 180    | 14     |
| 5      | 132    | 15     |
| 6      | 172    | 16     |
| 7      | 114    | 17     |
| 8      | 178    | 18     |
| 9      | 93     | 19     |
| 10     | 131    | 20     |

Table XIV

Steiner triple systems in homogeneous codes

| Index | # Index | Index | # Index |
|-------|---------|-------|---------|
| 1     | 3       | 9     | 36     | 17    | 10     |
| 2     | 23      | 10    | 36     | 19    | 9      |
| 3     | 15      | 11    | 27     | 22    | 8      |
| 4     | 63      | 12    | 7      | 25    | 19     |
| 5     | 36      | 13    | 26     | 26    | 19     |
| 7     | 5       | 14    | 18     | 29    | 7      |
| 8     | 60      | 16    | 6      | 61    | 4      |

Table XV

Sizes of sets of Steiner quadruple systems

| Size | # Size | Size | # Size |
|------|--------|------|--------|
| 1    | 101    | 11   | 91     |
| 2    | 97     | 12   | 142    |
| 3    | 77     | 13   | 142    |
| 4    | 180    | 14   | 109    |
| 5    | 132    | 15   | 41     |
| 6    | 172    | 16   | 94     |
| 7    | 114    | 17   | 38     |
| 8    | 178    | 18   | 59     |
| 9    | 93     | 19   | 31     |
| 10   | 131    | 20   | 17     |

IV. Structure of i-Components

Consider a binary one-error-correcting code $C$ and a nonempty subcode $D \subseteq C$. If we get another one-error-correcting code from $C$ by complementing coordinate $i$ exactly in the words belonging to $D$, then $D$ is said to be an $i$-component of $C$ and the operation is called switching. An $i$-component is minimal if it is not a superset of a smaller $i$-component. The reader is referred to [21] for a more thorough discussion of $i$-components.

Any process that transforms a perfect code into another by changing values in a single coordinate can be accomplished by switching, because the codewords that are changed form an $i$-component by definition. An extension followed by a puncturing can be viewed as such a process; hence all codes that have equal extension can be transformed into each other by switching.

The minimum distance graph of a code consists of one vertex for each codeword and one edge for each pair of codewords whose mutual distance equals the minimum distance of the code. All minimal $i$-components can be determined by a straightforward algorithm: for a prescribed value of $i$, construct the minimum distance graph and remove all edges but those connecting two codewords that differ in coordinate $i$. The connected components of this graph—for 1-perfect codes with length $n \geq 15$ there are at least two of them [21 Proposition 6]—form the minimal $i$-components of the code. The minimal $i$-components partition the code, and any $i$-component is a union of minimal ones.

The distribution of sizes of minimal $i$-components is presented in Table XVI. Each row lists the number of sets of given sizes as well as the number of such partitions (whose total number is $15 \cdot 5983 = 89745$). It has been known that partitions with 2 sets of size 1024 as well as 16 sets of size 128 exist, cf. [21].

As mentioned above, $i$-components and switching are means of constructing new codes from old ones. Codes that can be
obtained from each other by a series of switches (possibly in different coordinates) form a switching class. (Malyugin [22], [12] considers a more restricted set of transformations that partition the switching classes further.) By [23], the binary 1-perfect codes of length 15 are partitioned into at least two switching classes; we are now able to compute the exact structure of the switching classes.

There are 9 switching classes for the binary 1-perfect codes of length 15, and their sizes are 5,819, 153, 3, 2, 2, 1, 1, 1, and 1. In particular, this gives a method for obtaining codes with (full) rank 15, which have been hard to construct. The class with 5,819 codes in fact contains all codes with full rank, with (full) rank 1, which is isomorphic to PSL\(_2\), respectively. Both of the codes have an automorphism class with 5,819 codes in fact contains all codes with full rank, with (full) rank 15, which have been hard to construct. The class with 5,819 codes in fact contains all codes with full rank, with (full) rank 1, which is isomorphic to PSL\(_2\), respectively. Both of the codes have an automorphism class with 5,819 codes in fact contains all codes with full rank, with (full) rank 1, which is isomorphic to PSL\(_2\), respectively.

The two full-rank codes that are not in the switching class of the Hamming code have one more code in their switching class, a code with rank 14 (so one may say that all binary 1-perfect codes of length 15 can be obtained by known constructions). These two full-rank codes have kernels of size 2 and 4, and their automorphism groups have orders 336 and 672, respectively. Both of the codes have an automorphism group which is the direct product of the kernel and a group isomorphic to PSL(3, 2), which has order 168; this group partitions the coordinates into two orbits of size 7 and one of size 1. Indeed, note that PSL(3, 2) is the group of symmetries of the Hamming code of length 7.

One may generalize the concept of \(i\)-components to that of \(\alpha\)-components; see [24], [25], and their references. An \(\alpha\)-component, where \(\alpha \subseteq \{1, 2, \ldots, n\}\), is an \(i\)-component for all \(i \in \alpha\). We call an \(\alpha\)-component trivial if it is the full code or if \(|\alpha| = 1\). It turns out that nontrivial \(\alpha\)-components of the binary 1-perfect codes of length 15 consist of 1,024 codewords with \(|\alpha| \in \{2, 3\}\).

The authors are confident with the double-counting argument used in [2] for validating the classification of the binary 1-perfect codes of length 15; anyway, the fact that no new cases were encountered in the switching classes further reinforces this confidence.

### V. Defining Sets of 1-Perfect Codes

A defining set of a combinatorial object is a part of the object that uniquely determines the complete object. The term unique should here be interpreted in the strongest sense, that is, there should be exactly one way of doing this, not one way up to isomorphism.

Avgustinovich [26] gave a brief and elegant proof (which is repeated in [3]) of the following result.

**Theorem 3:** The codewords of weight \((n - 1)/2\) (alternatively, weight \((n + 1)/2\)) form a defining set of any binary 1-perfect code of length \(n\).

Avgustinovich and Vasil’eva [27] were further able to prove the following related result.

**Theorem 4:** The codewords of weight \(w\) with \(w \leq (n + 1)/2\) form a defining set for the codewords of weight smaller than \(w\) of any binary 1-perfect code of length \(n\).

One may ask whether it is possible to strengthen these results by proving that the codewords of weight \((n - 3)/2\) or any other weight smaller than \((n + 1)/2\) form a defining set for a binary 1-perfect code of length \(n\). We shall now prove that this is not possible in general. In fact, the theorem will be even stronger than that.

**Theorem 5:** The Hamming code of length \(n\) with \(n \geq 7\) has no defining set consisting of codewords all of whose weights differ from \((n - 1)/2\) and \((n + 1)/2\).

#### Proof of Theorem 5

The Hamming code of length \(n\) has a parity check matrix

\[
H = \begin{pmatrix}
0 & 1 & 1 \\
A & A & 0
\end{pmatrix},
\]

where \(A\) is a parity check matrix for the Hamming code of length \((n - 1)/2\) and 1 is an all-one vector. It can be easily checked that all words in the set

\[
S = \{(1 + x \cdot x |x|) : x \in F_2^{(n-1)/2}, \ A x = 0\}
\]

are codewords of the Hamming code if \(n \geq 7\); \(|x|\) is the weight of \(x\) modulo 2.

For an arbitrary word \(c \in S\), consider a word \(c'\) in the Hamming code such that \(d(c, c') = 3\) and \(c\) and \(c'\) differ in the last coordinate. Since two column vectors of \(H\) that add to \((1 \ 0)\) can only have the form \((0 \ a)\) and \((1 \ a)\), it follows that \(c' \in S\).

Consequently, \(S\) is an \(i\)-component with respect to the last coordinate, cf. Section [4]. A switch in this component produces a different code with changes made only to the last coordinate. Since the words of \(S\) have weight \((n - 1)/2\) considering all but the last coordinate, the transformed codewords (old and new) have only weights \((n - 1)/2\) and \((n + 1)/2\). Hence, no sets of codewords all weights of which differ from \((n - 1)/2\) and \((n + 1)/2\) can form a defining set for Hamming codes of length greater than or equal to 7.

For specific codes one can find examples of various defining sets. Examination of the classified codes of length 15 shows that there are cases where the codewords of weight 4 form a defining set but no cases where this holds for some weight smaller than 4 (this follows from Table [XI] and a consideration of the case where the smallest weight is 1, for which the words of weight 3 form a partial Steiner triple system). The existence of defining sets of weights 5 and 6 follows by using the result for weight 4 and Theorem 4. The cases of weights greater than 9 are analogous.

One interesting observation was made in the study of this property. Namely, there are binary 1-perfect codes of length
15, whose codewords of weight 7 are a proper subset of the codewords of the same weight in another code. In other words, this means that there are codes whose codewords of weight 7 form a defining set only under the assumption that this set of words contains all codewords of weight 7. This result can be generalized.

Theorem 6: Theorem [5] holds for \( n \geq 7 \) only under the assumption that the given set of codewords of weight \((n-1)/2\) (alternatively, weight \((n+1)/2\)) is complete.

Proof: We shall prove that there exist two perfect codes of length \( n \), \( C_1 \) and \( C_2 \), so that the codewords of weight \((n-1)/2\) of \( C_1 \) is a proper subset of those in \( C_2 \). We let \( C_1 \) be the Hamming code, defined by \( H \) as in the proof of Theorem [5].

Similarly to that proof, we consider \( i \)-components with respect to the last coordinate, but here we focus on the codewords in

\[ S = \{ (x \mid x) : x \in \mathbb{F}_2^{(n-1)/2}, Ax = 0 \}. \]

Analogously to the argument in the proof of Theorem [5], \( S \) is an \( i \)-component. If \( wt(x) \) is odd, then the weight of \((x \mid x)\) is odd (and there are such codewords with weight \((n-1)/2\)) and a switch produces a word with even weight. If \( wt(x) \) is even, say \( 2r \), then the weight of \((x \mid x)\) is \( 4v \) and after the switch it becomes \( 4v+1 \), and therefore cannot equal \((n-1)/2\), which is of the form \( 2^k - 1 \), for \( n \geq 7 \). Consequently, the codewords of weight \((n-1)/2\) of the new code \( C_2 \) obtained by the switch is a proper subset of the codewords with the same weight in \( C_1 \).

VI. SYSTEMATIC 1-PERFECT CODES

A binary code of size \( 2^k \) is said to be systematic if there are \( k \) coordinates such that the codewords restricted to these coordinates contain all possible \( k \)-tuples; otherwise it is said to be nonsystematic. It is known [28], [29] that nonsystematic binary 1-perfect codes exist for all admissible lengths greater than or equal to 15. It turns out that there are 13 nonsystematic binary 1-perfect codes of length 15 that extend to 12 nonsystematic codes.

The following invariant is closely related to the concept of systematic binary codes. The set

\[ ST(C) = \{ sup(x - y) : x, y \in C, d(x, y) = 3 \} \]

must obviously have size between \( \binom{2^k}{3}/3 \) (the size of a Steiner triple system of order \( n \)) and \( \binom{n}{3} \) when \( C \) is a binary 1-perfect code of length \( n \); for \( n = 15 \) these bounds are 35 and 455, respectively. The distribution of the values of \( |ST(C)| \) is shown in Table XVII for the 1-perfect codes of length 15.

Generalizing the concept of independent sets in graphs, a subset \( S \) of the vertices of a hypergraph is said to be independent if none of the edges is included in \( S \). Viewing \( ST(C) \) of a code \( C \) of length \( n = 2^m - 1 \) as a 3-uniform hypergraph, if the independence number of this graph—denoted by \( \alpha(C) \)—is smaller than \( m \), then \( C \) is nonsystematic [28]. In particular, if \( |ST(C)| = \binom{n}{3} \), then \( \alpha(C) = 2 \) and the code is nonsystematic.

Out of the 13 nonsystematic 1-perfect codes of length 15, six indeed have \( |ST(C)| = \binom{15}{3} = 455 \). Out of the others, six have \( |ST(C)| = 427 \) with \( \alpha(C) = 3 \), and one has \( |ST(C)| = 231 \) with \( \alpha(C) = 8 \). The distribution of the independence numbers of all codes, systematic as well as nonsystematic, is presented in Table XVIII.

Examples of nonsystematic binary 1-perfect codes of length 15 with \( |ST(C)| = 455 \) and \( |ST(C)| = 427 \) were earlier obtained in [29], and 12 inequivalent nonsystematic codes were encountered in [12]; see also [30]. The fact that there is a nonsystematic code \( C \) of length \( 2^m - 1 \) such that \( \alpha(C) > m \) shows that the above mentioned sufficient condition for a 1-perfect code \( C \) to be nonsystematic is not necessary, a question asked in [29].

For a binary 1-perfect code of length 15 with \( \alpha(C) = 8 \), let \( S \) be the complement of a maximum independent set. A counting argument shows that each \( STS(15) \) of the code contains 7 triples on \( S \), and hence each \( STS(15) \) contains an \( STS(7) \) on \( S \). Moreover, for the code with \( |ST(C)| = 231 \), \( ST(C) \) contains exactly those 3-subsets that intersect \( S \) in 1 or 3 coordinates. Also the 3-subsets for the codes with \( |ST(C)| = 427 \) have a combinatorial explanation: the missing
3-subsets form an STS(15) with one point and the blocks intersecting that point removed, in other words, a 3-GDD of type $2^7$.

VII. EMBEDDING ONE-ERROR-CORRECTING CODES

Avgustinovich and Krotov [31] show that any binary one-error-correcting code of length $m$ can be embedded (after appending a zero vector of appropriate length to the codewords) into a binary 1-perfect code of length $2^m - 1$. One may further ask for the shortest 1-perfect code into which such a code can be embedded. For example, any binary one-error-correcting code of length 4—thee are three inequivalent such codes, \{0000\}, \{0000, 1110\}, and \{0000, 1111\}—can be embedded into the (unique) 1-perfect code of length 7, but this does not hold for all codes of length 5 (because the Hamming code of length 7 does not contain a pair of codewords with mutual distance 5).

The occurrence of codes of length greater than or equal to 5 in the classified codes was checked. It turns out that for lengths 5 and 6, all inequivalent one-error-correcting codes can be found in a binary 1-perfect code of length 15, but not all such codes of length 7 can be found. Out of several examples, here is one code (of size 10) that is not embeddable in a binary 1-perfect code of length 15:

$00000000 00111100 01101110 01110111$

$10010011 10101110 10111010 11010101 11100011$

One could further consider the stricter requirement that a code should be embedded in a perfect code in such a way that it is not a subset of another embedded code. The construction in [31] indeed gives codes with this strong property. This requirement is rather restrictive as, for example, the code \{0000\} does not fulfill it with respect to the Hamming code of length 7.

The largest embedded codes with the property of not being subcodes of other embedded codes are directly related to certain fundamental properties. For example, a binary 1-perfect code of length $2^m - 1$ is systematic if and only if there exists an $m$-subset of coordinates for which the maximum size is 1. In other words, minimizing the maximum size over all $m$-subsets of coordinates should result in size 1. Instead maximizing the maximum size over subsets leads to the concept of cardinality-length profile (CLP), from which one may obtain the generalized Hamming weight hierarchy of a code; see [3].

For a code $C \subseteq F_2^n$, the cardinality-length profile $\kappa_i(C)$, $1 \leq i \leq n$, is defined as

$$\kappa_i(C) = \max_D \log_2 |D|,$$

where $D \subseteq C$ and all words in $D$ must coincide in $n - i$ coordinates. The profiles of the binary 1-perfect codes of length 15 are listed in Table XIX in the nonlogarithmic form $\kappa'_i(C), \kappa'_2(C), \ldots$, where $\kappa'_i(C) = 2^{|\kappa_i(C)|}$, together with the number of codes with such profiles.

The fact that the number of codes in the last row of Table XIX equals the number of binary 1-perfect codes of length 15 that do not have full rank is in accordance with [3 Corollary 4.7]. By [3 Proposition 4.5] we already know that $8 < \kappa'_i(C) < 16$; the new results reveal that $\kappa'_i(C)$ can attain every value in this interval except 9. The only other value of $i$ for which $\kappa'_i(C)$ may be different for codes that have and do not have full rank is $i = 6$; however, whereas $\kappa'_6(C) \in \{6, 7\}$ is only possible for full-rank codes, $\kappa'_6(C) = 8$ is possible for both types.

Also the cardinality-length profiles of the extended binary 1-perfect codes of length 16 are listed in nonlogarithmic form, in Table XX.

One more concept can be related to the discussion in this section. An OA$_\nu(t, k, q)$ orthogonal array of index $\lambda$, strength $t$, degree $k$, and order $q$ is a $k \times N$ array with entries from \{0, 1, \ldots, q-1\} and the property that every $t \times 1$ column vector appears exactly $\lambda$ times in every $t \times N$ subarray; necessarily $N = \lambda q^t$.

Binary 1-perfect codes of length 15 can be viewed as $15 \times 2048$ arrays and their extensions as $16 \times 2048$ arrays. It is then obvious from Tables XIX and XX that these are OA$_{10}(7, 15, 2)$ and OA$_{16}(7, 16, 2)$ orthogonal arrays, respectively. In fact, we shall prove (a general result) implying that there are no other orthogonal arrays with these parameters. The following result by Delsarte [33] is of central importance in the main proof.

Theorem 7: An array is an orthogonal array of strength $t$ if and only if the MacWilliams transform of the distance distribution of the code formed by the columns of the array has entries $A'_0 = 1, A'_1 = A'_2 = \cdots = A'_t = 0$.

For information on the MacWilliams transform in general and the application to orthogonal arrays in particular, see [1, Ch. 5] and [34, Ch. 4], respectively. With standard techniques—frequently used in a similar context, see, for example, [35], [36], [37]—one can now prove the following result; the part of the proof showing that these codes are orthogonal arrays can be found in several places, including [3, Theorem 4.4].

Theorem 8: Every OA$_\nu(t, n, 2)$ with $n = 2^m - 1$, $t = (n - 1)/2$, and $\lambda = 2^{2m-t-m}$ corresponds to a 1-perfect binary code of length $n$, and vice versa. Every OA$_\nu(t, n, 2)$ with $n = 2^m$ and $t$ and $\lambda$ as earlier corresponds to an extended 1-perfect binary code of length $n$, and vice versa.

Proof: Perfect codes and their extensions have a unique distance distribution. Therefore, the minimum distance of the dual of the (extended) Hamming code of length $n$ gives the (maximum possible) value of $t$ in Theorem 7 for any (extended) 1-perfect code. A simplex code with a minimum distance of $(n + 1)/2$ is the dual of a Hamming code, and a first order Reed-Muller code with a minimum distance of $n/2$ is the dual of an extended Hamming code. This shows that every (extended) 1-perfect code is an orthogonal array with the given parameters.

Going in the opposite direction, it is clear that the code obtained from the orthogonal array OA$_\nu(t, n, 2)$ with $n = 2^m - 1$, $t = (n - 1)/2$, and $\lambda = 2^{2m-t-m}$ has the length and cardinality of a 1-perfect code. Let $A'_t$ be the MacWilliams transform of the distance distribution of the code. By Theorem 7 we
This solution is the distribution of the Hamming code, so the minimum distance of the Hamming code. Thereby the code has length and size as an extended 1-perfect binary code—leads to an extended 1-perfect code.

By taking the MacWilliams transform of $A$, which together with $(2t+1)$ gives an OA of Theorem 2.24, an OA of $\lambda(t, n, 2)$ can be obtained from an OA of $\lambda(t, n, 2)$ and every OA of $\lambda(t, n, 2)$ can be used to construct an OA of $\lambda(t, n, 2)$. Application of Theorem 8 completes the proof.

**Corollary 9:** The number of isomorphism classes of $O\lambda(7, 15, 2)$ orthogonal arrays is 5983, and the number of isomorphism classes of $O\lambda(7, 16, 2)$ orthogonal arrays is 2165.

Classification results for some other related orthogonal arrays can also be obtained.

**Theorem 10:** Every $O\lambda(t, n, 2)$ with $n = 2^m - 2$, $t = (n - 3)/2$ and $\lambda = 2^{m-1}-m$ can be obtained by shortening a 1-perfect code, and every $O\lambda(t, n, 2)$ with $n = 2^m - 1$ and $t$ and $\lambda$ as earlier can be obtained by shortening an extended 1-perfect code.

**Proof:** By [34, Theorem 2.24], an $O\lambda(2t, k, q)$ can be obtained from an $O\lambda(2t+1, k+1, q)$ and any $O\lambda(2t, k, q)$ can be used to construct an $O\lambda(2t+1, k+1, q)$. Application of Theorem 8 completes the proof.

We now get two specific results using values calculated in [2].

**Corollary 11:** The number of isomorphism classes of $O\lambda(6, 14, 2)$ orthogonal arrays is 38408, and the number of isomorphism classes of $O\lambda(6, 15, 2)$ orthogonal arrays is 5983.
VIII. MIXED PERFECT CODES

The discussion in Section VII focuses on (the structure of) pairs of codewords with mutual distance 3. For a particular such structure, which we shall now discuss, one is able to construct perfect codes with both quaternary and binary coordinates. Moreover, since this construction is reversible, we obtain a complete classification of these codes.

Assume that there exist three coordinates of a binary 1-perfect code of length 15 such that all codewords can be partitioned into pairs of words that differ only in those coordinates. In other words, the kernel of the code has an element with 1s in exactly these three coordinates. The values of the pairs in the three coordinates are then \{000, 111\}, \{001, 110\}, \{010, 101\}, and \{100, 011\}. It is not difficult to verify that replacing each original pair of codewords with one codeword and the three coordinates by an element from the finite field \(\mathbb{F}_4\) (or any alphabet of size 4) gives a mixed 1-perfect code. This transformation is reversible, and has been used several times to construct good binary codes (of various types, both covering and packing) from codes with quaternary coordinates \([38], [39], [40]\).

Moreover, for any set of \(t\) elements in the kernel with weight 3 and disjoint supports, we can obtain a mixed 1-perfect code with \(t\) quaternary coordinates. By determining all possible mixed 1-perfect codes that can be obtained in this manner and carrying out isomorph rejection among these, we found that the number of inequivalent 1-perfect codes over \(\mathbb{F}_2^{15} \oplus \mathbb{F}_2^3\), \(\mathbb{F}_2^{12} \oplus \mathbb{F}_2^6\), \(\mathbb{F}_2^{12} \oplus \mathbb{F}_2^6\), and \(\mathbb{F}_2^5\) are 6,483, 39, 4, 1, and 1, respectively. Uniqueness of the quaternary 1-perfect code of length 5 has earlier been proved in [41]. The orders of the automorphism groups of these codes are listed in Tables XXI to XXVI (the existence of the codes is well known, for example, via the existence of the quaternary Hamming code of length 5 and the construction discussed above.)

| Table XXI | AUTOMORPHISM GROUPS OF 1-PERFECT CODES OVER \(\mathbb{F}_2^{15} \oplus \mathbb{F}_2^3\) |
|---|---|---|---|
| \([\text{Aut}(C)]\) | # | \([\text{Aut}(C)]\) | # |
| 8 | 1 | 168 | 11 | 24,576 | 8 |
| 16 | 12 | 1024 | 609 | 32,768 | 7 |
| 32 | 289 | 1536 | 22 | 49,152 | 3 |
| 64 | 1125 | 2048 | 343 | 65,536 | 2 |
| 96 | 1 | 3072 | 25 | 98,304 | 5 |
| 128 | 1447 | 4096 | 154 | 196,608 | 1 |
| 192 | 14 | 6144 | 12 | 294,912 | 1 |
| 256 | 1390 | 8192 | 64 | 589,824 | 1 |
| 384 | 14 | 12288 | 4 |  |
| 512 | 892 | 16384 | 26 |  |

The four code pairs of length 3 listed earlier are in fact cosets of the binary Hamming code of length 3, and the outlined construction is a special case of a general construction [39] that transforms coordinates over \(\mathbb{F}_{2^m}\) into cosets of the Hamming code of length \(2^m - 1\).

To transform a binary 1-perfect code of length 15 into a 1-perfect code over \(\mathbb{F}_8 \oplus \mathbb{F}_2^5\), we may search for a partition of the code into 128 subcodes of size 16 with all words in a subcode coinciding in 8 given coordinates. However, it turns out that this case can be proved in a direct way.

**Theorem 12:** There are exactly 10 inequivalent 1-perfect codes over \(\mathbb{F}_8 \oplus \mathbb{F}_2^5\).

**Proof:** Consider a 1-perfect code \(C\) over \(\mathbb{F}_8 \oplus \mathbb{F}_2^5\), such a code has size 128. Puncturing \(C\) in the 8-ary coordinate gives a binary code \(C'\) of length 8 and minimum distance at least \(3 - 1 = 2\). The code \(C'\) is unique, and consists of either all words of even weight or all words of odd weight.

Next consider the 8 subcodes \(C_i\) obtained by shortening in the 8-ary coordinate and taking all words whose 8-ary value is \(i\). The codes \(C_i\) have length 8 and minimum distance 4 (at least 3, but words in \(C'\) do not have odd mutual distances), and since the maximum number of codewords in a code with these parameters is 16, all codes \(C_i\) must have size 16 (16-8 = 128).

Consequently, the set of subcodes \(C_i\) form an extension of a partition of \(\mathbb{F}_2^5\) into binary 1-perfect codes of length 7. There are 10 inequivalent such extended partitions [42] and accordingly equally many inequivalent 1-perfect codes over \(\mathbb{F}_8 \oplus \mathbb{F}_2^5\).

The existence of 1-perfect codes over \(\mathbb{F}_8 \oplus \mathbb{F}_2^5\) has been known and follows, for example, from [43, Theorem 2]. The automorphism groups of these codes can be obtained from [42, Appendix] and are shown in Table XXVI.

No other 1-perfect codes over \(\mathbb{F}_2^1, \mathbb{F}_2^1 \oplus \mathbb{F}_2^1, \ldots, \mathbb{F}_2^m\) can be obtained from the binary 1-perfect codes of length 15, since...
any such code must have \( i_j + i_k \leq 4 \) for all \( 1 \leq j < k \leq n \) [44, Lemma 1].

IX. Various Other Properties

The current study focuses on properties of general interest; various other questions in the literature that can be addressed via the classified codes include those in [45] Sect. 8). We conclude the paper by discussing a few sporadic results and open problems.

Several (nontrivial) properties of perfect codes have earlier been proved analytically; we shall here briefly mention one such property. The minimum distance graph of a binary 1-perfect code of length 15 is a 35-regular graph of order 2048. Phelps and LeVan [23] ask whether inequivalent binary 1-perfect codes always have nonisomorphic minimum distance graphs. This question is answered in the affirmative by Avgustinovich in [46], building on earlier work by Avgustinovich and others [47], [48]. An analogous result is obtained for extended binary 1-perfect codes in [49], where it is also shown that the automorphism group of an (extended) binary 1-perfect code is isomorphic to the automorphism group of its minimum distance graph for lengths \( n \geq 15 \).

Let \( (n, M, d) \) denote a binary code of length \( n \), size \( M \), and minimum distance \( d \); such a code with the largest possible value of \( M \) with the other parameters fixed is called optimal. By shortening binary 1-perfect codes of length 15 up to \( i = 3 \) times we get optimal \((15 − i, 2^{11−i}, 3)\) codes. But do we get all such codes, up to equivalence, in this manner? For \( i = 1 \) we do, as shown in [50]: this result was used in [2] to classify the optimal \((14, 1024, 3)\) codes. But for \( i = 2 \) we do not, as shown in [51]. The general problem is, however, still open.

Two of the open problems stated in [3] still seem out of reach even for the case of binary 1-perfect codes of length 15.

The intersection number of two codes, \( C_1 \) and \( C_2 \), is \(|C_1 \cap C_2|\). The intersection number problem asks for the set of possible intersection numbers of distinct binary 1-perfect codes. Since binary 1-perfect codes are self-complementary, these intersection numbers are necessarily even. Among other things it is known that for binary 1-perfect codes of length 15, 0 (trivial) and 2 (by [3] Theorem 3.2]) are intersection numbers and in [14] Sect. III it is proved that the largest number is \( 2^{11} − 2^2 = 1920 \). Several other intersection numbers are known [52], but determining all possible intersection numbers seems challenging.

The proof of Theorem 12 relies on a classification [42] of partitions of \( \mathbb{F}_2^n \) into binary 1-perfect codes. This classification problem may be considered for \( \mathbb{F}_{2^5} \) as well, but even the restricted version (stated in [3]) with 16 equivalent codes in the partition seems hopeless.

Acknowledgments

The authors thank Olof Heden, Denis Krotov, Sergey Mal'yugin, Ivan Mogilnykh, Faina Solov'eva, Dmitrii Zinov'ev, Victor Zinov'ev, and the anonymous reviewers for their helpful comments. The proofs of Theorems 5 and 6 are based on comments by one of the referees.
