Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 187–192*

Perfect Trades of Small Length [1]

Denis Krotov krotov@math.nsc.ru
Sobolev Institute of Mathematics, Novosibirsk, Russia

Abstract. We classify inequivalent binary extended 1-perfect bitrades of length 10, constant-weight extended 1-perfect bitrades of length 12, and STS bitrades derived from them. As a corollary, we see that there is only one pair of disjoint Steiner sextuple systems $\mathrm{S}(5, 6, 12)$, up to equivalence. Keywords: bitrades, 1-perfect code, Steiner trades, small Witt design.

1 Introduction

Trades of different types are used to study, construct, and classify differect kinds of combinatorial objects (codes, designs, matrices, orthogonal arrays, etc.) and also studied independently, as some natural generalization of objects the corresponding type. In the current research, we classify small (extended) 1-perfect binary bitrades and STS bitrades derived from them. As a partial result of the classification, we find that there is only one, up to equivalence, pair of disjoint small Witt designs $\mathrm{S}(12, 6, 5)$ and it cannot be continued to a triple of disjoint $\mathrm{S}(12, 6, 5)$.

In our computer-aided classification, we used general principles described in [2]. The programs were written in `sage` [5], and `nauty` [4] was used to deal with automorphisms and isomorphisms.

2 Definitions

The graphs $G = (\mathrm{V}(G), \mathrm{E}(G))$ we consider are simple (without loops and multiple edges), connected, and regular. By the *distance* $\mathrm{d}(x, y)$ between two vertices x and y of a graph we mean the minimum length of a path connecting x and y. Two sets C and S of vertices of a graph are *equivalent* if there is an automorphism π of the graph such that $\pi(S) = C$. Two pairs (C_0, C_1) and (S_0, S_1) of sets of vertices of a graph are *equivalent* if there is an automorphism π of the graph such that either $\pi(S_0) = C_0$ and $\pi(S_1) = C_1$ or $\pi(S_0) = C_1$ and $\pi(S_1) = C_0$. The *automorphism group* $\mathrm{Aut}(C)$ of a vertex set is defined as its stabilizer in the graph automorphism group.

[1] The research was carried out at the expense of the Russian Science Foundation (Grant 14-11-00555).

2.1 Hamming graphs, halved n-cubes, and Johnson graphs

The *Hamming graph* $\mathrm{H}(n,q)$ (if $q = 2$, the *n-cube* $\mathrm{H}(n)$) is a graph whose vertices are the words of length n over the alphabet $\{0,\ldots,q-1\}$, two words being adjacent if and only if they differ in exactly one position. The *weight* $\mathrm{wt}(x)$ of a word x is the number of nonzeros in x. The *halved n-cube* $\frac{1}{2}\mathrm{H}(n)$ is a graph whose vertices are the even-weight (or odd-weight) binary n-words, two words being adjacent if and only if they differ in exactly two positions.

The *Johnson graph* $\mathrm{J}(n,w)$ is a graph whose vertices are the weight-w binary n-words, two words being adjacent if and only if they differ in exactly two positions. It is known that any automorphism of $\mathrm{H}(n)$, $\frac{1}{2}\mathrm{H}(n)$, or $\mathrm{J}(n,w)$ is a composition of a coordinate permutation and a translation to some word x, which is arbitrary in the case of $\mathrm{H}(n)$, even-weight for $\frac{1}{2}\mathrm{H}(n)$, the all-zero 0^n or all-one 1^n for $\mathrm{J}(2w,w)$, and only 0^n for $\mathrm{J}(n,w)$, $n \neq 2w$.

The *Hamming distance* $\mathrm{d_H}(x,y)$ between two words x and y of the same length denotes the number of coordinates in which x and y differ, i.e., the distance in the corresponding Hamming graph. Note that the graph distance in a Johnson graph or the halved n-cube is twice smaller than the Hamming distance: $\mathrm{d}(x,y) = \mathrm{d_H}(x,y)/2$.

2.2 1-perfect codes, extended 1-perfect codes, Steiner systems

A 1*-perfect code* is a set of vertices of $\mathrm{H}(n)$ such that every radius-1 ball contains exactly one codeword.

An *extended* 1*-perfect code* is a set of vertices of $\frac{1}{2}\mathrm{H}(n)$ such that every maximum clique contains exactly one codeword. Note that the maximum cliques in $\frac{1}{2}\mathrm{H}(n)$ are the radius-1 spheres in $\mathrm{H}(n)$ centered in odd-weight words. There is a one-to-one correspondence between the 1-perfect codes in $\mathrm{H}(n)$ and the extended 1-perfect codes in $\frac{1}{2}\mathrm{H}(n+1)$: if, for some fixed $i \in \{1,\ldots,n+1\}$, we delete the ith symbol from all codewords of an extended 1-perfect code, then the resulting set will be a 1-perfect code (inversely, the deleted symbol can be uniquely reconstructed as the modulo-2 sums of the other symbols). Extended 1-perfect codes in $\frac{1}{2}\mathrm{H}(n+1)$ (1-perfect codes in $\mathrm{H}(n)$) exist if and only if $n+1$ is a power of 2.

A *Steiner k-ple system* $\mathrm{S}k\mathrm{S}(n)$ (also abbreviated as $\mathrm{S}(k-1,k,n)$) is a set of vertices of $\mathrm{J}(n,k)$, $n \geq 2k$, such that every maximum clique contains exactly one word from the set ($\mathrm{S3S}(n)$ and $\mathrm{S4S}(n)$ are well known as $\mathrm{STS}(n)$ and $\mathrm{SQS}(n)$, Steiner triple systems and Steiner quadruple systems, respectively). Note that the maximum cliques in $\mathrm{J}(n,k)$ consists of all weight-k binary n-words adjacent in $\mathrm{H}(n)$ with a given word of weight $k-1$ (or of weight $k+1$, in the case $n = 2k$). It is straightforward that the weight-3 (weight-3) codewords of a 1-perfect (respectively, extended 1-perfect) code of length n form a $\mathrm{STS}(n)$ (respectively, $\mathrm{SQS}(n)$) if and only if the code contains the all-zero word 0^n. However, in contrast to the 1-perfect codes, $\mathrm{STS}(n)$s ($\mathrm{SQS}(n)$s) exist for all

$n \equiv 1, 3 \bmod 6$ (respectively, $n \equiv 2, 4 \bmod 6$).

The parameters $\mathrm{S}(5, 6, 12)$ play a special role in our classification. A sextuple system $\mathrm{S}(5, 6, 12)$ is unique up to equivalence and known as the *small Witt design*.

2.3 1-perfect, extended 1-perfect, Steiner bitrades

A 1-*perfect bitrade* ("bitrade" is a synonym of "2-way trade") is a pair (T_0, T_1) of disjoint nonempty sets of vertices of $\mathrm{H}(n)$ such that for every radius-1 ball B it holds

$$|B \cap T_0| = |B \cap T_1| \in \{0, 1\}. \tag{1}$$

An *extended* 1-*perfect bitrade* (SkS *bitrade*) is a pair (T_0, T_1) of disjoint nonempty sets of vertices of $\frac{1}{2}\mathrm{H}(n)$ ($\mathrm{J}(n, k)$ with $n \geq 2k$, respectively) such that for every maximum clique B of $\frac{1}{2}\mathrm{H}(n)$ ($\mathrm{J}(n, k)$), (1) holds.

In what follows, *bitrade* always means one of the three considered types of bitrades. Each component T_i of a bitrade (T_0, T_1) is called a *trade* (however, there is a different terminology in the literature, where (T_0, T_1) is called a trade, and each of T_0, T_1 are trade legs, or mates, or something else). The *volume* of a bitrade (T_0, T_1) is the cardinality of only one of T_0, T_1. The *length* of (T_0, T_1) means the length of words T_0 and T_1 consist of. A bitrade (T_0, T_1) is called *primary* if it cannot be partitioned into two bitrades (T_0', T_1') and (T_0'', T_1''), $T_0 = T_0' \cup T_0''$, $T_1 = T_1' \cup T_1''$. The role of bitrades in the study of (extended) 1-perfect codes, Steiner systems is emphasized by the following fact: if C_0 and C_1 are different 1-perfect codes, extended 1-perfect codes, or Steiner k-ple systems with the same parameters, then $(C_1 \backslash C_0, C_0 \backslash C_1)$ is a bitrade of the corresponding type.

Extended 1-perfect bitrades and 1-perfect bitrades are in the same one-to-one correspondence as extended 1-perfect codes and 1-perfect codes. If (T_0, T_1) is a 1-perfect or extended 1-perfect bitrade and $x \notin T_0, T_1$ is a word at distance k from T_0, then the weight-k words of $T_0 + x$ and $T_1 + x$ form an SkS bitrade, called *derived* from (T_0, T_1).

For bitrades consisting of words of weight $n/2$ (we call them *constant-weight* bitrades), there is the following simple but remarkable correspondence.

Proposition 1. *A pair (T_0, T_1) of weight-k binary $2k$-words is a SkS$(2k)$ bitrade if and only if it is an extended 1-perfect bitrade.*

A tuple $(T_0, \ldots, T_{k-1})$ of $k \geq 2$ sets is called a *k-way trade* if every two different sets from it form a bitrade. The concepts defined above for the bitrades (length, volume, primary, derived) and Proposition 1 are naturally extended to k-way trades.

2.4 Characteristic functions

By the characteristic function of a (1-perfect, extended 1-perfect, or SkS) bitrade (T_0, T_1) we will mean the function $\chi_{(T_0,T_1)} \stackrel{\text{def}}{=} \chi_{T_0} - \chi_{T_1}$, where χ_T denotes the characteristic $\{0,1\}$-function of a set T.

It is straightforward that the characteristic function of a (1-perfect, extended 1-perfect, or SkS) bitrade is an eigenfunction of the corresponding graph with the eigenvalue -1, $-n/2$, or $-k$, respectively. The graph $\mathrm{H}(n)$ has an eigenvalue -1 if and only if n is odd; $-n/2$ is an an eigenvalue of $\frac{1}{2}\mathrm{H}(n)$ if and only if n is even; $-k$ is an eigenvalue of all $\mathrm{J}(n,k)$s, $n \geq 2k$. For all these cases, bitrades are known to exist.

3 Auxiliary statements

The following fact is well known.

Lemma 1. *Let ϕ be an eigenfunction of $\mathrm{H}(n)$ with the eigenvalue $n-2i$, $i \in \{0,1,\ldots,n\}$. For every vertex x of $\mathrm{H}(n)$, it holds $\phi(x+1^n) = (-1)^i\phi(x)$, where 1^n is the all-one word.*

Corollary 1. *Let (T_0, T_1) be a (extended) 1-perfect bitrade in $\mathrm{H}(n)$ ($\frac{1}{2}\mathrm{H}(n+1)$, respectively).*

(i) If $n \equiv 3 \bmod 4$ ($0 \bmod 4$), then $T_0 = \overline{T}_0$ and $T_1 = \overline{T}_1$, where $\overline{T}_j = T_j + 1^n = \{x + 1^n \mid x \in T_j\}$.

(ii) If $n \equiv 1 \bmod 4$ ($2 \bmod 4$), then $T_0 = \overline{T}_1$.

We see that there is an essential difference between the cases (i) and (ii). In case (ii), T_1 is uniquely determined from T_0. They are complementary to each other and thus equivalent. In case (i), each element of a bitrade (T_0, T_1) is self-complementary, but T_0 does not uniquely define T_1 and vice versa. In fact, for every $n \equiv 1 \bmod 4$, there exists a 3-way trade. For $k > 3$, k-way trades can also exist.

The following easy-to-prove lemma plays a crucial role in our classification algorithm.

Lemma 2 ([3, Theorem 1])**.** *Suppose T_0, T_1 are disjoint vertex sets of $\frac{1}{2}\mathrm{H}(x)$ (or $J(n,w)$). The pair (T_0, T_1) is an extended 1-perfect trade (SkS trade, respectively) if and only if the subgraph induced by $T_0 \cup T_1$ is bipartite with parts T_0, T_1 and regular of degree $n/2$ (of degree k, respectively).*

4 Extended 1-perfect bitrades in $\frac{1}{2}\mathrm{H}(8)$

Before we classify the extended 1-perfect bitrades in $\frac{1}{2}\mathrm{H}(8)$, we note that this is the first nontrivial case. Indeed, if (T_0, T_1) is an extended 1-perfect bitrade in

$\frac{1}{2}\mathrm{H}(6)$, then we can assume without loss of generality that $T_0 \ni 000000$ and, in accordance with Lemma 2, $T_1 \ni 000011$, 001100, 110000; then, by Corollary 1, $T_0 = \{000000, 111100, 110011, 001111\} = T_1 + 1^6$.

Now consider three extended 1-perfect codes of length 8,
$C_0 = \langle 00001111, 00110011, 01010101, 11111111 \rangle$,
$C_1 = \langle 10000111, 00110011, 01010101, 11111111 \rangle$,
$C_2 = \langle 00001111, 00110101, 01010110, 11111111 \rangle$,
where $\langle \ldots \rangle$ denotes the linear span over the finite field of order 2. It is not difficult to check that $(C_0 \backslash C_1, C_1 \backslash C_0)$, $(C_0 \backslash C_2, C_2 \backslash C_0)$, and $(C_1 \backslash C_2, C_2 \backslash C_1)$ are constant-weight extended 1-perfect trades of volume 8, 12, and 14, respectively. As we see from the following theorem, all nonequivalent primary extended 1-perfect trades are exhausted by these three constant-weight trades and two trades of volume 16 (each consisting of two extended 1-perfect codes).

Theorem 1. *Up to equivalence, there are only* 5 *nonequivalent primary extended* 1*-perfect bitrades in* $\frac{1}{2}\mathrm{H}(8)$*, of volume* 8*,* 12*,* 14*,* 16 *and* 16*, respectively.*

5 Extended 1-perfect bitrades in $\frac{1}{2}\mathrm{H}(10)$

As the results of a computer-aided classification, there are 8 nonequivalent primary extended 1-perfect bitrades in $\frac{1}{2}\mathrm{H}(10)$, of volume 16, 24, 28, 32, 32, 32, 36, 40; the first 5 of them can be obtained from the 5 primary extended 1-perfect bitrades in $\frac{1}{2}\mathrm{H}(8)$ by the construction $(T_0, T_1) \to (T_0 01 \cup T_1 10, T_0 10 \cup T_1 01)$. The bitrades of volume 16, 24, 28, and 36 are constant-weight (the trades of the last one are optimal constant-weight codes); the other cannot be represented as constant-weight. Each trade of the bitrade of volume 40 is an optimal distance-4 code equivalent to the well-known Best code.

In Table 3.4. of [1], the authors list all nonequivalent STS bitrades of volume at most 9. As the result of the current search, we can say that the STS bitrades number 1 (of volume 4), 2, 4 (of volume 6), 5 (STS of volume 6), 7, 10, 11, 12, 13, 14, 15, 16 (of volume 8) are derived, 6 (of volume 7) and 10 (of volume 8) are not derived (numbers 3, 8, 9 are for 3- and 4-way trades), all STS bitrades of volume 9 are not derived from extended 1-perfect bitrades of length 10. Note that derived STS bitrades are not necessarily primary.

It should be noted that if an STS bitrade is derived from extended 1-perfect bitrades of length $n+1$ (10, in our case), and has at most n essential coordinates, then it is derived from 1-perfect bitrades of length n (9).

6 Extended 1-perfect bitrades in $\frac{1}{2}\mathrm{H}(12)$

It is hardly possible to enumerate all primary extended 1-perfect bitrades in $\frac{1}{2}\mathrm{H}(12)$ the same technique as for $\frac{1}{2}\mathrm{H}(10)$, even if we reject isomorphic partial solutions at some steps of the search. However, if we restrict the search by only the words of weight 6, the number of cases becomes essentially smaller and exhaustive enumeration becomes possible if we additionally apply the isomorph rejection. The isomorph rejection reduced the total time of the algorithm run by the factor 1400, approximately. All calculation took several days using one core of a modern personal computer.

The results of the classification are the following. Up to equivalence, there are exactly 25 constant-weight extended 1-perfect bitrades in $\frac{1}{2}\mathrm{H}(12)$ of the following volumes: 32, 48, 56, 56, 68, 86, 72, 72, 72, 72, 80, 80, 92, 92, 92, 96, 96, 98, 102, 108, 108, 110, 110, 120, 120, 132.

The bitrade of the maximum volume, 132, consists of two small Witt designs $\mathrm{S}(5,6,12)$. Only 7 nonequivalent bitrades, of volume 72, 96, 108, 108, 120, 120, 132, can be represented as the difference pair $(W_0\backslash W_1, W_1\backslash W_0)$ of two $\mathrm{S}(5,6,12)$ W_0 and W_1.

Corollary 2. *Up to equivalence, there is only one pair of disjoint $S(5,6,12)$.*

Four of bitrades, of volume 72, 108, 110, and 110, can be continued to 3-way trades (T_0,T_1,T_2); it occurs that for given T_0 and T_1, the choice of T_2 is unique; it follows that for the considered parameters, no primary bitrades can be continued to k-way trades for $k>3$. The 3-way trades from the bitrades of volume 110 are the same; so, there are only three nonequivalent 3-way trades obtained by continuing primary bitrades with considered parameters.

References

[1] A. D. Forbes, M. J. Grannell, and Griggs T. S. Configurations and trades in Steiner triple systems. *Australas. J. Comb.*, 29:75–84, 2004.

[2] P. Kaski and P. R. J. Östergård. *Classification Algorithms for Codes and Designs*, volume 15 of *Algorithms Comput. Math.* Springer, Berlin, 2006. DOI: 10.1007/3-540-28991-7.

[3] D. S. Krotov, I. Yu. Mogilnykh, and V. N. Potapov. To the theory of q-ary Steiner and other-type trades. E-print 1412.3792, arXiv.org, 2014. Available at http://arxiv.org/abs/1412.3792.

[4] B. D. McKay. nauty users guide (version 1.5). Technical Report TR-CS-90-02, Computer Science Department, Australian National University, Canberra, 1990.

[5] W. A. Stein et al. Sage Mathematics Software (Version 6.9), 2015. `http://www.sagemath.org`.