Small perfect trades

Denis Krotov

Sobolev Institute of Mathematics
Novosibirsk, Russia

ACCT 2016, June 18–24, Albena, Bulgaria

Trades

- Trades (bitrades) correspond to differences between two different objects of the same types (Steiner systems or other designs (and their q-ary generalizations, subspace designs), Latin squares or Latin hypercebes, perfect codes, MDS codes, MRD codes, orthogonal arrays, ...)
- If C' and C'' are two objects of the same parameters (e.g., STS(13)), then $(C' \backslash C'', C'' \backslash C')$ is a bitrade (each of $C' \backslash C''$, $C'' \backslash C'$ is a trade).
- However, the trades are defined independently of the existence of complete objects.

Steiner bitrades

- $S(t, k, v) \rightarrow$ Steiner (t, k, v) bitrade
  A Steiner (t, k, v) bitrade is difined as a pair (T_0, T_1) of disjoint block sets (where block is a k-subset of V) such that every t-subset is either included in exactly one block from T_0 and exactly one block from T_1 or not included in any block of $T_0 \cup T_1$.

(extended) 1-perfect bitrades

- 1-perfect code $\to$ 1-perfect bitrade
  A 1-perfect bitrade is difined as a pair (T_0, T_1) of disjoint vertex sets of $H(n, q)$ (or any other graph) such that every ball of radius 1 either has exactly one vertex from T_0 and one vertex from T_1 or disjoint with both T_0, T_1.
- extended 1-perfect binary code $\to$ extended 1-perfect bitrade
  An extended 1-perfect bitrade is difined as a pair (T_0, T_1) of disjoint sets of even-weight vertices of $H(n, 2)$ such that every sphere of radius 1 centered in an odd-weight vertex either has exactly one vertex from T_0 and one vertex from T_1 or disjoint with both T_0, T_1.

1-perfect trades and Steiner trades

Lemma

Let (T_0, T_1) be a 1-perfect or extended 1-perfect trade in $H(n, 2)$. Let k be the minimum weight of words of T_0 and T_1. Let T'_i denote the subset of T_i consisting of words of weight k. Then (T'_0, T'_1) is a Steiner $(k-1, k, n)$ trade.

Results

- Current result: we classify, up to equivalence, all extended 1-perfect trades in $H(8,2)$, $H(10,2)$, and $H(12,2)$ (in the last case, only the constant-weight trades, which also imply that they are $S(5,6,12)$ trades).
- Elements of the general theory: [D. S. Krotov, I. Yu. Mogilnykh, and V. N. Potapov. To the theory of q-ary Steiner and other-type trades.]

Context

General theory [K, Mogilnykh, Potapov]:

- We consider a rather general class of trades, which generalizes several known types of trades, including latin trades, Steiner $(k-1, k, v)$ trades, extended 1-perfect bitrades.
- We prove a characterization of trades in terms of subgraphs of the original graph and in terms of eigenfunctions.
- We prove a characterization of minimum (in the sence of the weight-distribution bound) trades in terms of isometric bipartite distance-regular subgraphs of the original distance-regular graph.

Def: eigenfunction, eigenvalues

An eigenfunction of a graph $\Gamma = (V, E)$ is a function $f : V \to \mathbb{R}$ that is not constantly zero and satisfies

$$\sum_{y \in \Gamma_1(x)} f(y) = \theta f(x) \tag{1}$$

for all x from V and some constant θ, which is called an eigenvalue of Γ.

(k, s, m) pairs

- Let Γ be a connected regular graph of degree k. Assume that S is a set of $(s+1)$-cliques in Γ such that every edge of Γ is included in exactly m cliques from S; in this case, we will say that the pair (Γ, S) is a (k, s, m) pair.
- Given a (k, s, m) pair (Γ, S), we define an S-design, or clique design, as a set of vertices that intersects with every clique from S in exactly one vertex. Examples of clique designs in distance-regular graphs: distance-2 MDS codes (Hamming graphs), distance-2 MRD codes (bilinear form graphs), STS, SQS, ..., $\mathrm{S}(k-1, k, v)$ (Johnson graphs), extended 1-perfect binary codes (halved n-cube), STS_q, $\mathrm{S}_q(k-1, k, v)$ (Grassmann graph).

Def: bitrade

- Let (Γ, S) be a (k, s, m) pair. A pair (T_0, T_1) of mutually disjoint nonempty vertex sets is called an S-bitrade, or a clique bitrade, if every clique from S either intersects with each of T_0 and T_1 in exactly one vertex or does not intersect with both of them (in particular, this means that each of T_0, T_1 is an independent set in Γ).
- A set of vertices T_0 is called an S-trade if there is another set T_1 (known as a mate of T_0) such that the pair (T_0, T_1) is an S-bitrade.
- Note that there are differences in terminology.
  We use "bitrade = (trade, trade)"
  not "trade = (leg, leg)".

A bitrade criterion

Theorem (K, Mogilnykh, Potapov, 2016)

Let (Γ, S) be a (k,s,m) pair. Let $T = (T_0, T_1)$ be a pair of disjoint nonempty independent sets of vertices of Γ. The following assertions are equivalent.

(a) *T is an S-bitrade.*

(b) *The function*

$$f^T(\bar{x}) = \chi_{T_0}(\bar{x}) - \chi_{T_1}(\bar{x}) = \begin{cases} (-1)^i & \text{if } \bar{x} \in T_i,\ i \in \{0,1\} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

is an eigenfunction of Γ with eigenvalue $\theta = -k/s$.

(c) *The subgraph Γ^T of Γ generated by the vertex set $T_0 \cup T_1$ is regular with degree $-\theta = k/s$ (as T_0 and T_1 are independent sets, this subgraph is bipartite).*

Calculating the weight distribution of an eigenfunction

Lemma

The weight distribution

$$W(x)=\left(\sum_{y\in\Gamma_0(x)}f(y),\ \sum_{y\in\Gamma_1(x)}f(y),\ \ldots,\ \sum_{y\in\Gamma_{\mathrm{diam}(\Gamma)}(x)}f(y)\right)$$

of an eigenfunction f of a distance-regular graph Γ is calculated as $(f(x)W^i_{A,\theta})_{i=0}^{\mathrm{diam}(\Gamma)}$ where the coefficients $W^i_{A,\theta}$ are derived from the intersection array $A=(b_0,\ldots,c_{\mathrm{diam}(\Gamma)})$ of Γ and the eigenvalue θ that corresponds to f.

Corollary (the weight-distribution (w.d.) bound)

An eigenfunction f of a distance-regular graph has at least $\sum_{i=0}^{\mathrm{diam}(\Gamma)}|W^i_{A,\theta}|$ nonzeros, in notation of the Lemma.

Trades that meet the w.d. bound

Theorem

Let Γ be a distance-regular graph. Let (Γ, S) be a (k, s, m) pair. Let $T = (T_0, T_1)$ be a pair of disjoint nonempty independent sets of vertices of Γ. The following are equivalent.

(a') *T is a minimum S-bitrade meeting the w.d. bound.*

(b') *The function f^T is an eigenfunction of Γ meeting the w.d. bound with eigenvalue $-k/s$.*

(c') *The subgraph Γ^T is a regular isometric subgraph of degree k/s. Moreover, Γ^T is distance regular.*

Example. Latin bitrades

- The vertex set of the Hamming graph $H(n, q)$ is the set $\{0, \ldots, q-1\}^n$ of words of length n over the alphabet $\{0, \ldots, q-1\}$. Two words are adjacent whenever they differ in exactly one position. The graph $H(n, 2)$ is also known as the n-cube, or the hypercube of dimension n.
- The clique designs in Hamming graphs are known as the latin hypercubes (in coding theory, these objects are known as the distance-2 MDS codes), and the clique bitrades, as the latin bitrades [1]. The most studied case, which corresponds to the latin squares, is $n = 3$, see e.g. [2].
- The bipartite distance-regular subgraph corresponding to a minimal bitrade is $H(n, 2)$.

---

[1] V. N. Potapov. Multidimensional Latin bitrades. *Sib. Math. J.*, 54(2):317–324, 2013.

[2] N. J. Cavenagh. The theory and application of latin bitrades: A survey. *Math. Slovaca*, 58(6):691–718, 2008.

Example. Steiner trades

- The vertices of the Johnson graph $J(n, w)$ are the binary words of length n and weight (the number of ones) w. Two words are adjacent whenever they differ in exactly two positions. The graphs $J(n, w)$ and $J(n, n - w)$ are isomorphic, and below we assume $2w \leq n$.
- The clique designs in Johnson graphs are known as the Steiner $\mathrm{S}(w - 1, w, n)$ systems, and the clique bitrades, as the Steiner $\mathrm{T}(w-1, w, n)$ bitrades. The subgraph corresponding to a minimal bitrade is $H(w, 2)$; an example of the vertex set of such subgraph is $\{(x, \bar{x}, 0, ..., 0) \mid x, \bar{x} \in \{0, 1\}^w, \ \bar{x}$ is opposite to $x\}$. The minimal bitrade cardinality was found in [3].
- In the case $w = 3$, the minimal trade is known as the Pasch configuration, or the quadrilateral.

[3] H. L. Hwang. On the structure of (v, k, t) trades. *J. Stat. Plann. Inference*, 13:179–191, 1986.

Example. Halved hypercube

- The vertices of the halved n-cube are the even-weight binary words of length n (i.e., a part of the bipartite n-cube). Two words are adjacent whenever they differ in exactly two positions.
- A maximal clique is the set of binary n-words adjacent in $H(n, 2)$ to a fixed odd-weight word. The clique designs in halved n-cubes are the extended 1-perfect codes. Such codes exist if and only if n is a power of two.
- The minimal cardinality of a bitrade is $2^{n/2}$. An example of a minimal bitrade is $\{(x, x) \mid x \in \{0, 1\}^{n/2}\}$; bitrades exist if and only if n is even. The graph corresponding to a minimum bitrade is $H(n/2, 2)$.

q-ary Steiner systems

- Let F_q^n be an n-dimensional vector space over the Galois field F_q of prime-power order q. The Grassmann graph $Gr_q(n,d)$ is defined as follows. The vertices are the d-dimensional subspaces of F_q^n. Two vertices are adjacent whenever they intersect in a $(d-1)$-dimensional subspace.
- All vertices that include a fixed $(d-1)$-dimensional subspace form a clique in $Gr_q(n,d)$; if $n \geq 2d$ then this clique is maximum. We form S from all such cliques.
- A set of vertices that intersects with every clique from S in exactly one vertex is known as a *q-ary Steiner* $\mathrm{S}_q[d-1,d,n]$ *system*. Constructing q-ary Steiner $\mathrm{S}_q[d-1,d,n]$ systems with $d \geq 3$ is not easy; at the moment, only the existence of $\mathrm{S}_2[2,3,13]$ is known in this field [M. Braun, at al. ArXiv: 1304.1462].
- An S-bitrade is called a Steiner $\mathrm{T}_q[d-1,d,n]$ bitrade.
- [DK,IM,VP,2016] The graph corresponding to a minimum bitrade is the dual polar graph $D_d(q)$ of order $\prod_{i=0}^{d-1}(q^i+1)$.

Computer-aided classification

Now, we return to the classification of extended 1-perfect bitrades of length 10.

Algorithm

- Below, we consider T_0 and T_1 as lists of words, whose contents changes during the run of the algorithm.
- At step 1, we assume that $T_0 \ni 0^{10}$ and $T_1 \ni v_1 = 1100000000$, $v_2 = 0011000000$, $v_3 = 0000110000$, $v_4 = 0000001100$, $v_5 = 0000000011$. Since any bitrade is equivalent to one with these words, these 6 words will not be changed during the search.
- At step 2, for i from $1, \ldots, 5$, we choose lexicographically first collection of 5 mutually non-adjacent words in the neighborhood of v_i satisfying the following property:
  —every chosen word is not adjacent to any known word of T_0
- and so on
- Use isomorph rejection

Validation of classification

- To check the results, we recount the number of solutions that should be found by the algorithm in alternative way. Double-counting is a standard way to validate computer-aided classifications of combinatorial objects, see [P. Kaski and P. R. J. Östergård. *Classification Algorithms for Codes and Designs*. 2006]
- If we have a bitrade (T_0, T_1), we know its automorphism group. Then we can calculate the number of equivalent objects and, in particular, the number of solutions the algorithm should find
- and check if this number is equal to the real number of found solutions.

Results: $n = 8, 10$

- For $n = 8$, there are trades of volume <u>8</u>, <u>12</u>, <u>14</u>, 16, 16. Each of them is the difference between two extended 1-perfect codes.
- For $n = 10$, there are trades of volume <u>16</u>, <u>24</u>, <u>28</u>, 32, 32, 32, <u>36</u>, 40. Five of them come from $n = 8$ by the construction

$$(T_0, T_1) \to (T_0 01 \cup T_1 10, T_0 10 \cup T_1 01)$$

.

- The bitrade of volume 36 consists of two optimal constant-weight codes;
- the bitrade of volume 40 consists of two optimal distance-4 codes (Best codes).

Results: $n = 12$

- For $n = 12$, there are constant-weight trades of volume 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. In the paper (arXiv:1512.03421) they can be bound with their automorphism groups and orbit representators.
- Four of bitrades, of volume 72, 108, 110, and 110, can be continued to 3-way trades (T_0, T_1, T_2).
- Only 7 nonequivalent bitrades, with volumes 72, 96, 108, 108, 120, 120, 132, can be represented as the difference pair $(W_0 \setminus W_1, W_1 \setminus W$ of two S(5, 6, 12) (Witt designs [R.D.Carmichael, 1931]) W_0 and W_1.

Examples

Bitrade of volume 32 (minimum):
Orbit representator: 01 01 01 01 01 01.
Automorphism group: the wreath product os S_6 and C_2.

Examples

Bitrade of volume 98:
Orbit representators:

$111111\,000000_{\times 2}$	$010101\,101010_{\times 2}$
$001110\,100011_{\times 6}$	$011100\,110001_{\times 6}$
$011011\,001001_{\times 6}$	$011100\,001110_{\times 6}$
$010110\,001101_{\times 6\cdot 2}$	$001011\,001011_{\times 12}$
$011010\,010110_{\times 6\cdot 2}$	$010110\,001011_{\times 12}$
$001100\,111001_{\times 12}$	$001011\,010110_{\times 12}$
$010100\,110101_{\times 12}$	$000001\,101111_{\times 12}$
$001010\,110101_{\times 12}$	$000101\,010111_{\times 12}$
$000101\,100111_{\times 12\cdot 2}$	$000101\,111001_{\times 12\cdot 2}$

Automorphism group: Dihedral group D_{12}:

$$\Big\langle (012345)(6789ab),\quad (0b)(1a)(29)(38)(47)(56) \Big\rangle$$

Examples

- Bitrades of volume 110 and 132 (maximum):
- Orbit representators (volume 110):
  T_0 : $000010111011_{\times 110}$
  T_1 : $000010011111_{\times 110}$
  T_2 : $000011110011_{\times 110}$
- Orbit representators (volume 132):
  T_0 : $00000101111\,1_{\times 132}$
  T_1 : $11110100000\,1_{\times 132}$
- Automorphism group:
  $\Big\langle (0123456789a)\ \ (13954)(267a8)\ \ (0b)(1a)(25)(37)(48)(69) \Big\rangle$
  $\sim PSL_2(11)$

Examples

Bitrade of volume 108:

Orbit representators: T_0 : $\begin{array}{|cccc|} \hline 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ \hline \end{array}$, $\begin{array}{|cccc|} \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ \hline \end{array}$

Automorphism group:

$$A_4 \times S_3$$

Tools

Programming language: SAGE
isomorphism, automorphisms: NAUTY