

On the number of latin bitrades of order 3

Vladimir N. Potapov (joint work with Denis S. Krotov)

Sobolev Institute of Mathematics, Novosibirsk, Russia

3rd Hungarian-Russian Combinatorics workshop,

Moscow, May 20 - 25, 2019

Definitions

A trade, broadly speaking, is the difference between two combinatorial structures with the same parameters. Trades, bitrades, unitrades are used for investigation and construction (via switching method) of combinatorial designs, latin squares, error-correcting codes and other structures.

A **latin unitrade** of order k is a set of vertices of the Hamming graph $H(n, k)$ that intersects with every maximal clique in even number of vertices. A **bitrade** is a bipartite unitrade with 0 or 2 vertices in every maximal clique, that is, a bitrade splittable into two independent sets. Latin bitrades correspond to the symmetric differences between two MDS codes or the differences between two latin hypercubes.

A set of all unitrades (indicator functions of unitrades) is a vector space over $GF(2)$. Therefore it is not difficult to calculate the number of all unitrades. It is equal to $2^{(k-1)^n}$.

There are two nonequivalent nonempty 2-dimensional unitrades of order 3 (in $H(2, 3)$).

0	1	1
0	1	1
0	0	0

0	1	1
1	0	1
1	1	0

Each 2-dimensional unitrade is a bitrade (Hall's theorem).

Examples

Example of 3-dimensional unitrade that is not a bitrade.

1	1	0	0	1	1	1	0	1
1	0	1	1	0	1	0	0	0
0	1	1	1	1	0	1	0	1

Example of 3-dimensional bitrade of order 3.

0	1	1	0	1	1	0	0	0
0	1	1	1	0	1	1	1	0
0	0	0	1	1	0	1	1	0

The asymptotic (as $n \rightarrow \infty$) of the number of n -dimensional bitrades of order $k > 2$ is unknown.

Main results

lower bound

The number $N'(n)$ of nonequivalent n -dimensional bitrades of order 3 is not less than $2^{(2/3-o(1))n}$ as $n \rightarrow \infty$.

upper bound

The number $N(n)$ of n -dimensional bitrades of order 3 is at most $2^{\alpha n}$, $\alpha < 2$, as $n \rightarrow \infty$.

n	$N'(n)$	$N(n)$	$\ln N(n)$	$\ln \ln N(n)$
0	2	3	1.098	0.094
1	2	7	1.945	0.665(+0.571)
2	3	31	3.433	1.233(+0.567)
3	5	403	5.998	1.791(+0.557)
4	13	29875	10.304	2.332(+0.541)
5	92	32184151	17.286	2.849(+0.517)
6	25493	1488159817231	28.028	3.333(+0.483)
7	> 2187260868	6171914027409468739	43.266	3.767(+0.434)

lower bound

Let vertices of $H(n, 3)$ be n -tuples over alphabet $Q_3 = \{-1, 0, 1\}$, i.e. $V(H(n, 3)) = Q_3^n$.

Introduce notations $\{0, \pm 1\}_0 = \{0, 1\}$, $\{0, \pm 1\}_1 = \{1, -1\}$, $\{0, \pm 1\}_{-1} = \{0, -1\}$ and $\{0, \pm 1\}_v = \{0, \pm 1\}_{v_1} \times \cdots \times \{0, \pm 1\}_{v_n}$.

A set of functions $\chi_{\{0, \pm 1\}_v}$ is a basis of latin unitrades as a vector space over $GF(2)$.

Each latin unitrade U is a linear combination

$$\chi_{U(A)} = \bigoplus_{v \in A \subset Q_3^n} \chi_{\{0, \pm 1\}_v}.$$

Proposition

If all pairwise Hamming distances between vertices of $A \subset Q_3^n$ are odd then $U(A)$ is a bitrade.

Proposition

There exists a equidistant code $C \subset Q_3^m$ with code distance 3^{t-1} and $|C| = 2m + 1 = 3^t$, where $m = \frac{3^t - 1}{2}$.

C is a dual code of the ternary Hamming code.
Every subset of C generates a latin bitrades.

Let \mathcal{A} be a set of functions $f : Dom \rightarrow Im$. A set $T \subset Dom$ is called **testing set for \mathcal{A}** if for each $f, g \in \mathcal{A}$ an equation $f|_T = g|_T$ implies $f = g$.

Proposition

If there exists a unitrade $U \subset Q_3^m$ that is not a symmetric difference between two bitrades then there exists a testing set $T \subset Q_3^m$ for indicators of bitrades with cardinality $|T| = 2^m - 1$.

Computer found such 7-dimensional unitrade of order 3.

Proposition

If there exist a testing set T for m -dimensional bitrades of order 3 then the number of km -bitrades of order 3 is at most $2^{|T|^k}$.

Therefore the number of bitrades in Q_3^{7k} is not greater than $2^{\alpha^{7k}}$, where $\alpha = (2^7 - 1)^{1/7} < 2$.

Krotov D.S, Potapov V.N. On the cardinality spectrum and the number of latin bitrades of order 3. arXiv:1812.00419 [math.CO] (in Russian)