# A Lower Bound on the Number of Boolean Functions with Median Correlation Immunity

Vladimir N. Potapov

*Sobolev Institute of Mathematics, Novosibirsk, Russia*

XVI International Symposium "Problems of Redundancy

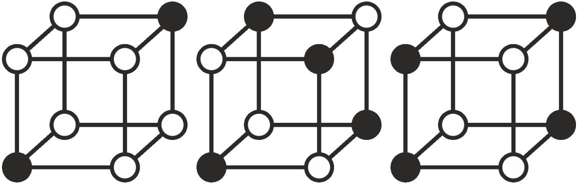
in Information and Control Systems", Moscow, October 21 – 26, 2019

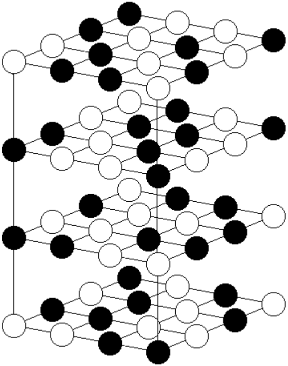
# Definitions

A set $Q_q^n = \{0, 1, \ldots, q-1\}^n$ with Hamming metric is called an $n$-dimensional hypercube. A hypercube is called Boolean if $q = 2$. A subset of $Q_q^n$ consisting of $n$-tuples with fixed values in fixed $(n-m)$ coordinates is called $m$-dimensional face ($m$-face).

A function $f : Q_q^n \to \{0, 1\}$ is called correlation immune of order $r$ if it takes the value 1 the same number of times for each $(n-r)$-face of the hypercube. A correlation immune function is called balanced (a resilient function) if it takes values 0 and 1 the same number of times.

# Examples





# History

O.V. Denisov, Discrete Math. Appl., vol. 2(4), 1992.
E.R. Canfield et al., Cryptogr. Commun, vol. 2, 2010.
K.N. Pankov, Discrete Math. Appl., vol. 29(3), 2019.

$N(n,k)$ is the number of resilient $n$-variable Boolean functions of order $k = const$.

$$N(n,k) \sim 2^{2^n+Q-k}(2^{n-1}\pi)^{-(M-1)/2},$$

where $M = \sum_{j=0}^{k} \binom{n}{j}$, $Q = \sum_{j=0}^{k} j\binom{n}{j}$.

Y. Tarannikov,"On the structure and numbers of higher order correlation-immune functions," Proceedings of IEEE International Symposium on Information Theory. 2000.

# Main results

The lower bound $2^{2^{n/2}}$ follows from a simple construction. Suppose that $n = 2m$. Consider an arbitrary Boolean function $f : Q_2^m \to Q_2$. Define a function $F : Q_2^{2m} \to Q_2$ by the equation $F(x, y) = f(x) \oplus |y|$, where $|y|$ is the parity of the Hamming weight of $y$. It is clear that $F$ takes values 0 and 1 the same number of times in each face with unfixed coordinate $y_i$, $i = 1, \ldots, m$.

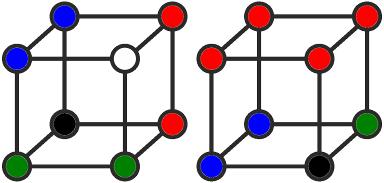
**Theorem**

There exist at least $n^{2^{(n/2)-1}(1+o(1))}$ different resilient $n$-variable Boolean functions of order $\frac{n}{2} - 1$.

$$N(n, \frac{n}{2}) \geq n^{2^{(n/2)-2}(1+o(1))}.$$

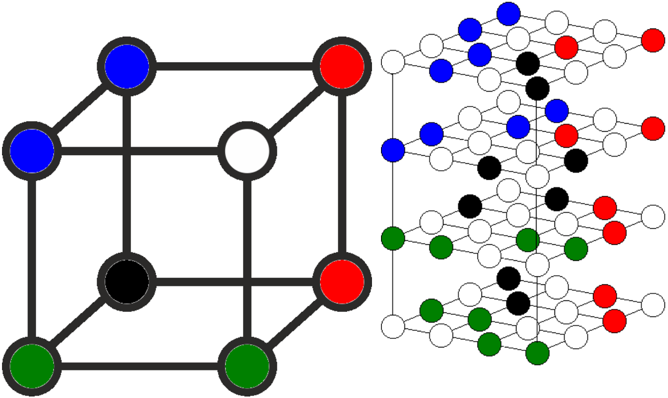
### Lemma 1

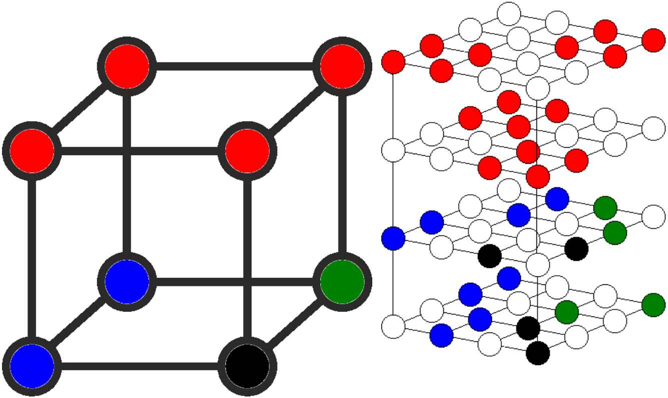
The number of splittings of $Q_2^n$ into pairwise nonintersecting faces is equal to $n^{2^{n-1}(1+o(1))}$.



**Lemma 2**

Different splittings of $Q_2^n$ correspond to different resilient functions $f : Q_4^n \rightarrow Q_2$ of order $n - 1$.





### Theorem

There exist at least $n^{2^{n-1}(1+o(1))}$ different resilient $2n$-variable Boolean functions of order $n-1$.

### Proof

Define an arbitrary bijection $\varphi : Q_2^2 \to Q_4$. Suppose $f : Q_4^n \to Q_2$ is a resilient function of order $n-1$. Define function $F : Q_2^{2n} \to Q_2$ by equation $F(x, y) = f(\varphi(x_1, y_1), \ldots, \varphi(x_n, y_n))$. Consider an arbitrary $(n+1)$-dimensional face $\Gamma$. There exists $i \in \{1, \ldots, n\}$ such that the pair of coordinates $(x_i, y_i)$ is not fixed in $\Gamma$. Since $f$ takes each of the values 0 and 1 two times in any 1-dimensional face of $Q_4^n$, $F$ takes each of the values 0 and 1 the same number of times in $\Gamma$.