S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 4, стр. 133–135 (2007) УДК 519.172.2
MSC 05C15

A BOUND ON CORRELATION IMMUNITY

D.G. FON-DER-FLAASS

ABSTRACT. A new bound on correlation immunity of non-constant unbalanced Boolean functions is proved. The bound is applied to obtain a new necessary condition for existence of a perfect coloring of the hypercube with given parameters. The new bound is stronger than the bounds previously obtained by Bierbrauer and Tarannikov, and is reached on an infinite class of examples.

In this note we prove a new bound on correlation immunity of unbalanced Boolean functions. This bound was conjectured by Yu. Tarannikov.

Let $\Omega = \{1, \ldots, n\}$. The powerset $H = \mathcal{P}(\Omega)$ will be considered as the n-dimensional hypercube; two subsets being adjacent iff they differ in exactly one element. For any sets x, y their symmetric difference will be denoted by $x + y$, and the size of x by $|x|$.

For $x, y \in H$, $x \cap y = \emptyset$, define the set $[x] + y = \{z \cup y \mid z \subseteq x\}$. This is just a k-dimensional face of the hypercube, where $k = |x|$.

Our main object is the 2^n-dimensional linear space V of all real-valued functions on H endowed with the standard inner product $\langle f, g\rangle = \sum_{x \in H} f(x)g(x)$. Also, by fg we denote the ordinary product of functions.

For any subset $S \subseteq H$, let χ^S be the characteristic function of S; that is, $\chi^S(x) = 1$ if $x \in S$, otherwise $\chi^S(x) = 0$.

Definition 1. *A function $f \in V$ is called correlation immune of degree $n - m$ iff $\langle f, \chi^U\rangle$ is constant for all m-dimensional faces $U \subseteq H$.*

Two special cases of this notion are particularly important and well-studied: correlation immune Boolean functions, and orthogonal arrays (for instance, cf. [6] and

FON-DER-FLAASS, D.G., A BOUND ON CORRELATION IMMUNITY.

The research was partially supported by the RFBR (grants 05-01-00816 and 06-01-00694).
Received April, 3, 2007, published April, 24, 2007.

[1]). A Boolean function is correlation immune of degree $n-m$ if the characteristic function of its set of ones is such, in our sense. An orthogonal array $OA_\lambda(t,k,2)$ can be defined as a multiset of binary vectors of length k intersecting every $(k-t)$-face by exactly λ elements (with multiplicities). So, it can be represented as a function taking integer non-negative values which is correlation immune of degree $k-t$.

The constant Boolean functions trivially are correlation immune of degree n. If a Boolean function is *balanced*, that is, it takes the value 1 in precisely one half of the cases, then its correlation immunity can be as large as $n-1$: consider the function $p(x) = |x| \bmod 2$. For non-constant unbalanced Boolean functions, non-trivial upper bounds for the correlation immunity were found in [1] and [6].

We shall prove here a bound which is stronger than all those proved earlier. This bound was conjectured by Yu. Tarannikov (private communication), and proved for $m \leq 4$ ([5]).

Theorem 1. *If the function χ^S for $S \subseteq H$, $\emptyset \neq S \neq H$, is correlation immune of degree $n-m$, and $|S| \neq 2^{n-1}$, then $m \geq n/3+1$.*

PROOF. Let $|S| = c$, and $|H \setminus S| = b = 2^n - c$. We have $b \neq 0$, $c \neq 0$, and $b \neq c$. Consider the function $q = b\chi^S - c\chi^{H\setminus S}$ (that is, $q(x) = b$ if $x \in S$, and $q(x) = -c$ otherwise). The function q is correlation immune of degree $n-m$, because χ^S is; and the sum of its values is 0. Therefore, $\langle q, \chi^U\rangle = 0$ for every face U of dimension m or more.

For every $x \in H$, define the function f^x as follows:

$$f^x(z) = (-1)^{|z\setminus x|}.$$

The collection $\{f^x \mid x \in H\}$ is an orthogonal basis of V (the Fourier basis). We can note that each f^x is an eigenvector of the adjacency matrix of the hypercube, with the eigenvalue $-n+2|x|$.

We shall need the following easy properties of the functions f^x.

(i) $f^\Omega \equiv 1$;

(ii) $f^x = \sum_{z\cap x=\emptyset}(-1)^{|z|}\chi^{[x]+z}$;

(iii) $f^x f^y = f^{x+y+\Omega}$.

Expand q on the basis $\{f^x\}$: $q = \sum w_x f^x$. Since the basis is orthogonal, we have

$$w_x = \frac{\langle q, f^x\rangle}{\langle f^x, f^x\rangle}.$$

It follows from (ii) and the correlation immunity of q that $w_x = 0$ if $|x| \geq m$.

Now consider the function q^2. Each value of q (b and $-c$) satisfies the equation $t^2 - (b-c)t - bc = 0$; therefore $q^2 = (b-c)q + bc \cdot f^\Omega$; so,

$$q^2 = bcf^\Omega + \sum_{x\in H}(b-c)w_x f^x.$$

On the other hand, using (iii), we find:

$$q^2 = (\sum_{y\in H} w_y f^y)(\sum_{z\in H} w_z f^z) = (\sum_{y,z\in H} w_y w_z f^{y+z+\Omega}) = (\sum w_y^2)f^\Omega + \sum_{y\neq z} w_y w_z f^{y+z+\Omega}.$$

Let k be the largest size of $x \in H$ for which $w_x \neq 0$. Take any x with $w_x \neq 0$; let $l = |x|$. Comparing coefficients at f^x in the above sums, we see that there exist $y \neq z$ such that $w_y \neq 0$, $w_z \neq 0$, and $y + z = x + \Omega$. Therefore, $n - l = |x + \Omega| = |y + z| \leq |y| + |z| \leq 2k$, and $n \leq l + 2k \leq 3k$. On the other hand, $k \leq m-1$, and the theorem is proved.□

What happens when equality is achieved? All the inequalities in the above proof also must turn into equalities, which means that $m = k + 1$, $n = 3k$, and every x for which $w_x \neq 0$, is of size k. So the function q, being a linear combination of eigenfunctions to the same eigenvalue $-3k + 2k = -k$, is itself such eigenfunction.

Take an arbitrary vertex $v \in S$, let it be adjacent to r elements of S and s elements of $H \setminus S$. We have two equations, $r + s = n$, and $br - cs = -kb$; the second one follows from q being an eigenfunction. Therefore r and s are uniquely determined, and do not depend on the choice of $v \in S$. Similarly, for some uniquely determined numbers t and u, every vertex $v \in H \setminus S$ has t neighbours in S and u neighbors in $H \setminus S$.

This means, by definition, that the partition $(S, H \setminus S)$ is an *equitable partition*, or a *perfect coloring*, of the hypercube (cf. [3] or [2]). Conversely, if the partition $(S, H \setminus S)$ is a perfect coloring with parameters (r, s, t, u) (where $r + s = t + u = n$) then the function $f \in V$ taking the value s on S, and the value $-t$ on $H \setminus S$ is an eigenfunction to the eigenvalue $r - t$, and so is correlation immune of degree $n - k + 1$, for $k = (n + r - t)/2 = r + (s - t)/2$. So, for perfect colorings our bound $n \leq 3k$ can be stated as follows:

Theorem 2. *If the partition $(S, H \setminus S)$ is a perfect coloring with parameters (r, s, t, u) where $s \neq t$ then $r \geq (3t - s)/4$.*

Three infinite families of examples achieving the equality are known. Two of them have the above parameters $(r, s, t, u) = (0, 3k, k, 2k)$ (cf. [4]), and one has the parameters $(r, s, t, u) = (l, 5l, 3l, 3l)$ (cf. [7]).

Acknowledgement. I am very grateful to Yu. Tarannikov for introducing me to the conjecture, for providing some relevant references, and for useful comments.

References

[1] J. Bierbrauer, *Bounds on orthogonal arrays and resilient functions*, Journal of Combinatorial Designs, **3** (1995), 179–183.

[2] D. Fon-Der-Flaass, *Perfect colorings of a hypercube*, to appear in Siberian Math. J.

[3] C. Godsil, *Equitable partitions*, in: Combinatorics, Paul Erdős is Eighty (Vol. 1). Keszthely (Hungary), 1993, 173–192.

[4] D. Kirienko, *On new infinite family of high order correlation immune unbalanced Boolean functions*, Proceedings of 2002 IEEE International Symposium on Information Theory ISIT'2002. Lausanne, Switzerland, June 30 - July 5, 2002, P. 465.

[5] Tarannikov Yu., Kirienko D., *Spectral analysis of high order correlation immune functions*, Proceedings of 2001 IEEE International Symposium on Information Theory ISIT'2001. Washington, DC, USA, June 2001, P. 69.

[6] Tarannikov Yu., Korolev P., Botev A.*Autocorrelation coefficients and correlation immunity of Boolean functions*, Proceedings of Asiacrypt 2001. Gold Coast, Australia, December 9-13, 2001. Lect. Notes in Comp. Sci. Springer-Verlag, **2248** (2001), 460–479.

[7] Tarannikov Yu., *On resilient Boolean functions with maximal possible nonlinearity*, Cryptology ePrint archive (`http://eprint.iacr.org`), Report 2000/005, March 2000, 18 p.

Dmitri Fon-Der-Flaass
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: `d.flaass@gmail.com`