Discrete Applied Mathematics 227 (2017) 70–83

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Bisecting binomial coefficients

Eugen J. Ionaşcu [a,*], Thor Martinsen [b], Pantelimon Stănică [b]

[a] Department of Mathematics, Columbus State University, Columbus, GA 31907, USA
[b] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5212, USA

ARTICLE INFO

Article history:
Received 4 January 2017
Received in revised form 22 April 2017
Accepted 26 April 2017
Available online 25 May 2017

Keywords:
Binomial coefficients
Subset sum problem
Diophantine equations

ABSTRACT

In this paper, we deal with the problem of bisecting binomial coefficients. We find many (previously unknown) infinite classes of integers which admit nontrivial bisections, and a class with only trivial bisections. As a byproduct of this last construction, we show conjectures Q2 and Q4 of Cusick and Li (2005). We next find several bounds for the number of nontrivial bisections and further compute (using a supercomputer) the exact number of such bisections for $n \leq 51$.

Published by Elsevier B.V.

1. Introduction

In the pursuit of constructing symmetric Boolean functions with various cryptographic properties (resilience, avalanche features), Mitchell [19], Gopalakrishnan et al. [13], von zur Gathen and Roche [11], as well as Cusick and Li [6], among others, study a seemingly "innocent" problem, namely the binomial coefficients bisection (BCB), which we shall describe below.

The connection between symmetric Boolean functions and binomial coefficients is rather immediate. Let $\mathbb{V}_n$ be an n-dimensional vector space over the two-element field $\mathbb{F}_2$. A Boolean function $f : \mathbb{V}_n \to \mathbb{F}_2$ is symmetric if its output value $f(\mathbf{x})$ only depends upon the (Hamming) weight of its input, $\mathrm{wt}(\mathbf{x})$ (number of nonzero bits of $\mathbf{x}$). Since there are $\binom{n}{w}$ vectors $\mathbf{x}$ of weight $\mathrm{wt}(\mathbf{x}) = w$, then f is constant on each such set of vectors, and so, f can be "compressed" into an $n + 1$ vector of values corresponding to each partition class of cardinality $\binom{n}{w}$, $0 \leq w \leq n$. Now, if one further imposes balancedness on f (in addition to symmetry), that is its weight is $\mathrm{wt}(f) = 2^{n-1}$, then it follows that one also has to have a two set partition I, J, of these binomial coefficients $\binom{n}{w}$ so that the function f has value $b \in \{0, 1\}$ on the vectors of weight in I and value $\bar{b}$ on vectors in J. Thus, we are prompted in studying these splitting (bisections) of binomial coefficients, and that is the subject of this paper.

If $\sum_{i=0}^{n} \delta_i \binom{n}{i} = 0$, $\delta_i \in \{-1, 1\}$, then we call $[\delta_0, \ldots, \delta_n]$ a solution of the (BCB) problem. So, the (BCB) problem consists in finding all these solutions (the set of all solutions will be denoted by $\mathcal{J}_n$) and in particular the number of all such solutions, which we will be denoted by J_n. Certainly, for such a solution, letting $I = \{i \mid \delta_i = 1\}$ and $J = \{i \mid \delta_i = -1\} := \bar{I}$, we obtain a *bisection* $\sum_{i \in I} \binom{n}{i} = \sum_{i \in J} \binom{n}{i} = 2^{n-1}$. Conversely, having a bisection we can reconstruct the solution of (BCB), that it came from, in the previous construction. So, in what follows we are going to use either one of the these descriptions of a solution of the (BCB) problem.

By the binomial theorem $\sum_i (-1)^n \binom{n}{i} = (1 - 1)^n = 0$, so $\pm[1, -1, 1, -1, \ldots]$ is always a solution of (BCB), i.e., we have at least two solutions for every n ($J_n \geq 2$). We also observe (see also [6]) that if n is odd then

$$[\delta_0, \ldots, \delta_{(n-1)/2}, -\delta_{(n-1)/2}, \ldots, -\delta_0]$$

* Corresponding author.
E-mail addresses: math@ejionascu.ro (E.J. Ionaşcu), tmartins@nps.edu (T. Martinsen), pstanica@nps.edu (P. Stănică).

http://dx.doi.org/10.1016/j.dam.2017.04.035
0166-218X/Published by Elsevier B.V.

with $\delta_i \in \{-1, 1\}$ arbitrary chosen, give $2^{(n+1)/2}$ solutions (that include the ones we mentioned before, so $J_{2n-1} \geq 2^n$). These are all called *trivial* solutions [6].

There are sporadic situations when nontrivial solutions do appear. For instance, when $n \equiv 2 \pmod 6$, because of the identity

$$\binom{n}{k} = 2\binom{n}{k-1} = \binom{n}{k-1} + \binom{n}{n-k+1},$$

where $k = \frac{n+1}{3}$ being odd, nontrivial solutions appear by moving the above terms from the equality

$$\sum_{i\ odd} \binom{n}{i} = \sum_{i\ even} \binom{n}{i},$$

from one side to the other. For example, if $n = 8$ we have

$$1 + \underline{28} + 70 + \underline{28} + 1 = 8 + \underline{56} + 56 + 8 \Rightarrow 1 + \underline{56} + 70 + 1 = 8 + \underline{28} + \underline{28} + 56 + 8.$$

This implies that $[1, -1, -1, 1, 1, -1, -1, -1, 1]$ is a solution for (BCB) problem. Besides these types of examples, all that is known about the bisection of binomial coefficients, are mostly computational results (see [6,11,13,19]).

2. A general approach and an upper bound

The well-known formula from trigonometry

$$\cos\alpha \cos\beta = \frac{1}{2}[\cos(\alpha+\beta) + \cos(\alpha-\beta)],\ \ \alpha, \beta\ \in \mathbb{R},$$

can be generalized easily (by induction on the number of angles) in the following way. For $x_1, x_2, \ldots, x_m$ arbitrary real numbers, we have

$$\cos x_1 \cos x_2 \cdots \cos x_m = \frac{1}{2^{m-1}} \sum \cos(x_1 \pm x_2 \pm \cdots \pm x_m),$$

where the sum is over all possible choices of signs +and −. This shows that the number of solutions (all possible choices of signs) of the equation $x_1 \pm x_2 \pm \cdots \pm x_m = 0$ (where x_i's are positive integers) is given by the formula

$$\frac{2^{m-1}}{2\pi} \int_{-\pi}^{\pi} \cos(x_1 t)\cos(x_2 t)\cdots\cos(x_m t) dt,$$

or, since the integrant is an even function,

$$\frac{2^{m-1}}{\pi} \int_{0}^{\pi} \cos(x_1 t)\cos(x_2 t)\cdots\cos(x_m t) dt.$$

Changing the variable, $t = \pi s$, we can apply this to the bisection of binomial coefficients, and immediately infer the next formula for J_n.

Theorem 1. *The number of binomial coefficients bisections for fixed n can be computed with the following formula*

$$J_n = 2^{n+1} \int_0^1 \prod_{j=0}^{n} \cos\left(\pi \binom{n}{j} s\right) ds. \tag{1}$$

We certainly could have used the below result of Freiman [10] (see also [1,4,5,7]; seemingly, Drimbe [7] was unaware of Freiman's work), but we preferred our elementary approach. We mention it here, though, since we will need it later in the paper.

Theorem 2. *Let $A = \{a_1, a_2, \ldots, a_N\}$ and $b \leq \frac{1}{2}\sum_{i=1}^{N} a_i$. The number of Boolean solutions for the equation*

$$\sum_{i=1}^{N} a_i x_i = b,\ \ x_i \in \{0, 1\}$$

is precisely $\int_0^1 e^{-2\pi i x b} \prod_{j=1}^{N} \left(1 + e^{2\pi i x a_j}\right) dx$.

Let us denote by $ES(x_1, x_2, \ldots, x_m)$ the number of all solutions of the equation $\pm x_1 \pm x_2 \pm \cdots \pm x_m = 0$. As we have shown, we have

$$ES(x_1, x_2, \ldots, x_m) = \frac{2^m}{\pi} \int_0^{\pi} \prod_{j=1}^{m} \cos\left(x_j t\right) dt. \tag{2}$$