2016-10-10

Bisecting binomial coefficients

Ionaşcu, Eugen J.

Monterey, California: Naval Postgraduate School

Bisecting binomial coefficients

Eugen J. Ionaşcu[1], Thor Martinsen[2], Pantelimon Stănică[2]

[1]Department of Mathematics,
Columbus State University
Columbus, GA 31907
Email: {math}@ejionascu.ro

[2]Department of Applied Mathematics,
Naval Postgraduate School
Monterey, CA 93943-5212, U.S.A.
Email: {tmartins,pstanica}@nps.edu

October 10, 2016

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 [7]. We next find several bounds for the number of nontrivial bisections and further compute (using a supercomputer) the exact number of such bisections for $n \leq 51$.

Keywords: Binomial coefficients, subset sum problem, diophantine equations.

1 Introduction

In the pursuit of constructing symmetric Boolean functions with various cryptographic properties (resilience, avalanche features), Mitchell [24], Gopalakrishnan et al. [16], von zur Gathen and Roche [14], as well as Cusick and Li [7], 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. Thus, 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 denoting by J_n. Certainly, for such a solution, letting $I = \{i \,|\, \delta_i = 1\}$ and $J = \{i \,|\, \delta_i = -1\} := \overline{I}$, 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 [7]) that if n is odd then

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

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 [7].

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 type of examples, all that is known about the bisection of binomial coefficients, are mostly computational results (see [24, 16, 14, 7]).

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, ..., 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*

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

We certainly could have used the below result of Freiman [11] (see also [1, 4, 5, 8]; seemingly, Drimbe [8] 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 $\displaystyle\int_0^1 e^{-2\pi i x b}\prod_{j=1}^{N}\left(1+e^{2\pi i x a_j}\right)d\,x.$

Let us denote by $ES(x_1, x_2, ..., x_m)$ 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

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

In [27, p. 441], it is shown that for every $k \in \mathbb{N}$, we have the formula

$$\int_0^{\pi/2}(\sin t)^k dt = \int_0^{\pi/2}(\cos t)^k dt = \begin{cases} \frac{(k-1)!!}{k!!}\frac{\pi}{2} \text{ if } k \text{ is even} \\ \\ \frac{(k-1)!!}{k!!} \text{ if } k \text{ is odd,} \end{cases}$$

where $k!! = k(k-2)\cdots$ (the product of all integers $\leq k$ having the same parity as k).

A generalization of the Integral Hölder Inequality can be stated in the following way: given f_1, f_2,..., f_m functions in $L^{2m}(X)$ (X is a measure space) we have

$$||\prod_{j=1}^{m} f_j||_2 \leq \prod_{j=1}^{m}||f_j||_{2m},$$

where $\|\cdot\|_p$ is the usual p-norm on the measure space X.
Putting these two ingredients together and using Cauchy-Schwartz Inequality, we obtain

$$\begin{aligned} ES(x_1,x_2,...,x_m) &\leq \frac{2^m}{\pi}\int_0^\pi \prod_{j=1}^m |\cos(x_j t)|\,dt \\ &\leq \frac{2^m}{\sqrt{\pi}}\left[\int_0^\pi \prod_{j=1}^m |\cos(x_j t)|^2 dt\right]^{1/2} \\ &\leq \frac{2^m}{\sqrt{\pi}}\prod_{j=1}^m \left(\int_0^\pi |\cos(x_j t)|^{2m}\right)^{1/(2m)} dt. \end{aligned}$$

But for $x_j \in \mathbb{N}$, we have

$$\begin{aligned} \int_0^\pi |\cos(x_j t)|^{2m} dt &= \frac{1}{x_j}\int_0^{x_j\pi} |\cos s|^{2m} ds = \int_0^\pi |\cos s|^{2m} ds \\ &= 2\int_0^{\pi/2} |\cos s|^{2m} ds = \frac{(2m-1)!!}{(2m)!!}\pi \end{aligned}$$

Hence, we obtained the following result.

Theorem 3. *Given x_1, x_2, ..., x_m arbitrary positive integers, the following estimates hold*

$$ES(x_1,x_2,...,x_m) \leq 2^m\left(\frac{(2m-1)!!}{2m!!}\right)^{1/2} = \left(2\binom{2m-1}{m}\right)^{1/2}. \tag{3}$$

In particular,

$$J_m \leq \left(2\binom{2m+1}{m+1}\right)^{1/2}.$$

Remark 4. *We know already that there are more than $2^{(n+1)/2}$ bisections for odd n and at most 2^{n+1} possible choices. Our Theorem 3 implies that the quotient between the solutions set size and the size of possible solutions space is $\frac{1}{\sqrt{\pi(n+1)/2}} \to 0$, as $n \to \infty$, which certainly was expected.*

2.1 A more detailed analysis

We start with the case of n odd. As in [2] we will be using the inequality

$$|\cos(\pi x)|^2 \leq \exp(-\pi^2\|x\|^2),$$

which is valid for all real x, where $\|x\|$ is the distance to the nearest integer. For easy writing, for n fixed, we let $b_j = \binom{n}{j}$ and $B = \lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$, n odd. Thus,

$$\begin{aligned} 2^{-(n+2)}J_n &= \frac{1}{2}\int_0^1 \prod_{j=0}^n \cos\left(\pi x\binom{n}{j}\right) = \int_0^{1/2}\prod_{j=0}^B \cos^2\left(\pi x\binom{n}{j}\right) \\ &\leq \int_0^{\frac{1}{2b_B}}\prod_{j=0}^B \cos^2\left(\pi x\binom{n}{j}\right)dx + \int_{\frac{1}{2b_B}}^{\frac{1}{2b_{B-1}}}\prod_{j=0}^{B-1}\cos^2\left(\pi x\binom{n}{j}\right)dx \\ &+ \cdots + \int_{\frac{1}{2b_1}}^{\frac{1}{2b_0}}\prod_{j=0}^0 \cos^2\left(\pi x\binom{n}{j}\right)dx. \end{aligned} \tag{4}$$

Observe now that, if $\frac{1}{2b_{k+1}} \leq x \leq \frac{1}{2b_k}$, then $\frac{b_j}{2b_{k+1}} \leq xb_j \leq \frac{b_j}{2b_k} \leq \frac{1}{2}$, if $j \leq k$, therefore, $\|xb_j\| = xb_j$, and so, with $B = \lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$ and $S_{n,s} := \sum_{j=0}^{B-s} \binom{n}{j}^2$, we have

$$\begin{aligned}\prod_{j=0}^{k} \cos^2(\pi x\ b_j)\, dx &\leq \prod_{j=0}^{k} \exp\left(-\pi^2 \|xb_j\|\|^2\right) = \prod_{j=0}^{k} \exp\left(-\pi^2 (xb_j)^2\right) \\ &= \exp\left(-\pi^2 x^2 \sum_{j=0}^{k} b_j^2\right) = \exp\left(-\pi^2 x^2 S_{n,B-k}\right).\end{aligned} \tag{5}$$

Certainly $S_{n,B-k} = \binom{2n}{n} - \binom{n}{k+1} {}_3F_2[1, k+1-n, k+1-n; k+2, k+2; 1]$, using the incomplete sum of powers of binomials coefficients (see [17]) in terms of the hypergeometric function, but unfortunately this is simply a rewrite of the expression, and will not be very useful in our analysis.

We now let, as it is customary, $\operatorname{erf}(z) = \frac{2}{\sqrt{\pi}} \int_0^z e^{-t^2} dt = \frac{2ze^{-z^2}}{\sqrt{\pi}} {}_1F_1\left(1; \frac{3}{2}; z^2\right)$, where ${}_1F_1$ is Gauss' hypergeometric function. It is also known that for $z \gg 1$ (recall that $k!!$ is the double factorial),

$$\operatorname{erf}(z) = \pi^{-1/2}\, \gamma\left(\frac{1}{2}, z^2\right) = 1 - \frac{e^{-z^2}}{\sqrt{\pi}} \sum_{k=0}^{\infty} \frac{(-1)^k (2k-1)!!}{2^k} z^{-2k-1},$$

where $\gamma(a, z) = \int_0^z t^{a-1} e^{-t} dt$ is the lower incomplete gamma function. In particular, under $z \gg 1$, we have (see [3], or any book on probabilities)

$$1 - \frac{e^{-z^2}}{z\sqrt{\pi}} \left(1 - \frac{1}{2z^2} + \frac{3}{4z^4}\right) \leq \operatorname{erf}(z) \leq 1 - \frac{e^{-z^2}}{z\sqrt{\pi}}. \tag{6}$$

Using the inequalities $e^x \geq 1 + x + \frac{x^2}{2}$, $e^{-x} \leq 1 - x + \frac{x^2}{2}$ and integrating we can find a better bound, but again, in the interest of simplicity, we roughly bound the decreasing function inside the integral and obtain (assume $0 < s \leq B$)

$$\begin{aligned}&\int_{\frac{1}{2b_{B-s+1}}}^{\frac{1}{2b_{B-s}}} \exp\left(-\pi^2 x^2 S_{n,s}\right) dx = \frac{\operatorname{erf}\left(\frac{\pi\sqrt{S_{n,s}}}{2b_{B-s}}\right) - \operatorname{erf}\left(\frac{\pi\sqrt{S_{n,s}}}{2b_{B-s+1}}\right)}{2\sqrt{\pi}\sqrt{S_{n,s}}} \\ &\leq \exp\left(-\frac{\pi^2 S_{n,s}}{4b_{B-s+1}^2}\right)\left(\frac{1}{2b_{B-s}} - \frac{1}{2b_{B-s+1}}\right)\end{aligned} \tag{7}$$

We now need to estimate (7). While it is known [9] (see also, Polya and Szegö [25, Vol. 1, Prob. 40, P. 42]) that

$$\sum_{j=0}^{n} \binom{n}{j}^r \sim \left(2^n \sqrt{\frac{2}{\pi n}}\right)^r \sqrt{\frac{\pi n}{2r}},$$

as well as the asymptotic for the incomplete sum of powers of binomials (we let $I := \{j \in \mathbb{N} \,|\, -a\sqrt{\frac{n}{4}} + \frac{n}{2} \leq j \leq a\sqrt{\frac{n}{4}} + \frac{n}{2}\}$)

$$\sum_{j \in I} \binom{n}{j}^r \sim 2^{nr} \sqrt{\frac{n}{4}} \left(\frac{\pi n}{2}\right)^{-r/2} \int_{-a+\frac{2}{\sqrt{n}}}^{-a+\frac{2}{\sqrt{n}}} e^{-rt^2/2} dt,$$

again, in the interest of simplicity, letting $\alpha_s := \frac{n}{\lfloor \frac{n}{2} \rfloor - s}$, we prefer to use the estimate $\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor - s} \binom{n}{k} = 2^{n(H(\alpha_s)+o(1))}$, where $H(\alpha) = -\alpha \log_2(\alpha) - (1-\alpha)\log_2(1-\alpha)$ is the binary entropy function, which easily implies the inequality $\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor - s} \binom{n}{j} < 2^n e^{-2s^2/n}$ for $0 \le s \le \lfloor \frac{n}{2} \rfloor$, rendering the bounds for $S_{n,s} = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor - s} \binom{n}{j}^2$,

$$\frac{1}{B-s+1}\left(\sum_{k=0}^{\frac{n}{2}-s}\binom{n}{k}\right)^2 < S_{n,s} < \binom{n}{\lfloor \frac{n}{2} \rfloor - s}\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor - s}\binom{n}{j} < 2^n e^{-\frac{2s^2}{n}}\binom{n}{\lfloor \frac{n}{2} \rfloor - s},$$

or the simpler

$$\frac{1}{B+1}2^{2n(H(\alpha_s)+o(1))} \le \frac{1}{B-s+1}2^{2n(H(\alpha_s)+o(1))} < S_{n,s} < 2^n e^{-\frac{2s^2}{n}}\binom{n}{\lfloor \frac{n}{2} \rfloor - s},$$

the lower bound being obtained by the Cauchy-Schwarz inequality. We can certainly remove the dependence on $o(1)$ by using the inequalities

$$\frac{1}{\sqrt{8n\alpha_s(1-\alpha_2)}}2^{nH(\alpha_s)} \le \sum_{k=0}^{\frac{n}{2}-s}\binom{n}{k} \le 2^{nH(\alpha_s)}.$$

Thus, (7) becomes (using $\binom{n}{k+1} - \binom{n}{k} = \frac{n-2k}{k+1}\binom{n}{k}$)

$$\begin{aligned}
&\int_{\frac{1}{2b_{B-s+1}}}^{\frac{1}{2b_{B-s}}} \exp\left(-\pi^2 x^2 S_{n,s}\right) dx \le \exp\left(-\frac{\pi^2 2^{2n(H(\alpha_s)+o(1))}}{4(B+1)b_{B-s+1}^2}\right)\frac{b_{B-s+1}-b_{B-s}}{2b_{B-s}b_{B-s+1}} \\
&\le \exp\left(-\frac{\pi^2 2^{2n(H(\alpha_s)+o(1))}}{4(B+1)b_{B-s+1}^2}\right)\frac{n-2B+2s-1}{2(B-s+1)b_{B-s+1}} \\
&= \exp\left(-\frac{\pi^2 2^{2n(H(\alpha_s)+o(1))}}{4(B+1)b_{B-s+1}^2}\right)\frac{s}{(B-s+1)b_{B-s+1}}.
\end{aligned}$$

We next estimate our integral on $[0, \frac{1}{2b_B}]$, and use the known identity $\sum_{j=0}^{\lfloor n/2 \rfloor}\binom{n}{j}^2 = \binom{2n}{n}$. Thus,

$$\begin{aligned}
&\int_0^{\frac{1}{2b_B}} \prod_{j=0}^{B} \cos^2(\pi x b_j)\, dx \le \int_0^{\frac{1}{2b_B}} \prod_{j=0}^{B} \exp\left(-\pi^2 \|x b_j\|^2\right) dx \\
&= \int_0^{\frac{1}{2b_B}} \exp\left(-\pi^2 x^2 \sum_{j=0}^{B} b_j^2\right) = \int_0^{\frac{1}{2b_B}} \exp\left(-\pi^2 x^2 \binom{2n}{n}\right) \\
&= \frac{\operatorname{erf}\left(\frac{\pi\sqrt{\binom{2n}{n}}}{2b_B}\right)}{2\sqrt{\pi\binom{2n}{n}}} \le \frac{1}{2\sqrt{\pi\binom{2n}{n}}}\left(1 - \frac{2b_B}{\pi\sqrt{\pi\binom{2n}{n}}}\exp\left(-\frac{\pi^2\binom{2n}{n}}{4b_B^2}\right)\right),
\end{aligned}$$

using (6).

Next, we consider the case of n being even, but n is not a power of 2 (this will be treated in the next section). Under this assumption, we see that $v_2\left(\binom{n}{n/2}\right) \geq 4$.

As before, for n fixed, we let $b_j = \binom{n}{j}$ and $B = \lfloor \frac{n}{2} \rfloor = \frac{n}{2}$, n even. Since $\cos\left(\pi x \binom{n}{n/2}\right) = 0$ for $x = \frac{2k+1}{2\binom{n}{n/2}}$, $k \in \mathbb{Z}$, we see that the expression inside the integral of J_n, namely, $\cos\left(\pi x \binom{n}{n/2}\right) \prod_{j=0}^{n/2-1} \cos^2\left(\pi x \binom{n}{j}\right)$ is positive for x in $\left[0, \frac{1}{2\binom{n}{n/2}}\right) \cup \left(\frac{3}{2\binom{n}{n/2}}, \frac{5}{2\binom{n}{n/2}}\right) \cup \cdots \cup \left(\frac{\binom{n}{n/2}-1}{2\binom{n}{n/2}}, \frac{1}{2}\right]$, and negative in $\left(\frac{1}{2\binom{n}{n/2}}, \frac{3}{2\binom{n}{n/2}}\right) \cup \left(\frac{5}{2\binom{n}{n/2}}, \frac{7}{2\binom{n}{n/2}}\right) \cdots$. Thus, J_n is the area on the first set of intervals minus the area on the second set of intervals. Using this observation, we see that the method we used for the case of n odd applies here, as well, and the bound remains the same (with the obvious change for B).

Putting all these estimates together, we thus obtain the following result (by abuse, we include the case of Hamming weight 1, since the bound of Theorem 7 is stronger in that case).

Theorem 5. *Let $\alpha_s = \frac{n}{\lfloor \frac{n}{2} \rfloor - s}$, $n \geq 5$. Then*

$$2^{-(n+2)} J_n \leq \frac{\operatorname{erf}\left(\frac{\pi\sqrt{\binom{2n}{n}}}{2\binom{n}{\lfloor n/2 \rfloor}}\right)}{2\sqrt{\pi\binom{2n}{n}}} + \sum_{s=1}^{\lfloor n/2 \rfloor - 1} \exp\left(-\frac{\pi^2 2^{2n(H(\alpha_s)+o(1))}}{4(\lfloor n/2 \rfloor + 1) b^2_{\lfloor n/2 \rfloor - s + 1}}\right) \frac{s}{(\lfloor n/2 \rfloor - s + 1) b_{\lfloor n/2 \rfloor - s + 1}}.$$

Remark 6. *With a little more work, one can find that the expression above is $O\left(\frac{2^n}{n}\right)$ (in fact, $J_n \leq \frac{2^{n+2}}{n}$).*

3 The 2^n case

We now treat the case of binomial coefficients corresponding to a power of 2.

Theorem 7. *If $N = 2^n$, $n \geq 3$, then $J_N \leq 0.3258 \cdot 2^{3 \cdot 2^{n-2} - 2^{\frac{n-3}{2}}}$, as $n \to \infty$.*

Proof. We first recall Kummer's result (see also, the paper by Granville [18]), which states that the p-adic valuation (p is a prime number) of a binomial coefficient (for any N, k) is

$$v_p\left(\binom{N}{k}\right) = \sum_i \frac{k_i + h_i - N_i}{p-1},$$

where N_i, k_i, h_i are the digits of $N, k, N-k$, respectively, in their base p representations. Equivalently, $v_p\left(\binom{n}{k}\right)$ is the number of *borrows* when subtracting k from N in base p (a result of Kummer rediscovered by Goetgheluck [15]). When $N = 2^n$ and $n, k \geq 1$, this reveals that

$$v_2\left(\binom{2^n}{k}\right) + v_2(k) = n. \tag{8}$$

It may be useful to visualize our method. The 2-adic valuation of the row of the Pascal's triangle corresponding to $N = 2^{2m}$ is the merging of the k-th rows corresponding to the binomial coefficients $\binom{2^n}{2^k(2s+1)}$, $s \geq 0$. Observe that every row will have twice as many entries as the one above, disregarding 0-th row corresponding to the endpoints with the 2-adic valuations $0, 0$, occurring at halves of the intervals above, starting with the 2-adic valuation of the middle binomial $\binom{2^{2m}}{2^{2m-1}}$. For example, if $n = 4$, then the tableaux of 2-adic valuations is

$$\begin{array}{cccccccccccccccc}
0 & & & & & & & & & & & & & & & 0 \\
& & & & & & & & 1 & & & & & & & \\
& & & & 2 & & & & & & & & 2 & & & \\
& & 3 & & & & 3 & & & & 3 & & & & 3 & \\
4 & & 4 & & 4 & & 4 & & 4 & & 4 & & 4 & & 4 & \\
\end{array} \tag{9}$$

which, by merging will become

$$\left\{ v_2\left(\binom{2^4}{k} \right) \right\}_{k=0}^{16} = \{0, 4, 3, 4, 2, 4, 3, 4, 1, 4, 3, 4, 2, 4, 3, 4, 0\}.$$

While we conjecture that if n is even, the only possible bisections are (for $n = 2m$) $B_1 = \left\{ \binom{2^n}{2k} \right\}_{k=0}^{2^{n-1}-1}$ and $B_2 = \left\{ \binom{2^n}{2k+1} \right\}_{k=0}^{2^{n-1}}$, we are unable to show that, but we will use an inductive procedure and show that every row (of our visual aid interpretation), except possibly for the last two rows belong to the same "bin", say B_1, of a bisection.

For easy writing, for n fixed, we let $b_k := \binom{2^n}{k}$. Since $v_2(b_0) = v_2(b_{2^n}) = 0$, then it is obvious that the endpoint binomial coefficients occur in the same "bin", say, B_1, otherwise, the sums of both of these bins is not even, let alone being equal to 2^{n-1}. We now let $b_0, b_{2^n} \in B_1$.

Next, we argue that for $n \geq 2$, $b_0, b_{2^{n-1}}, b_{2^n}$ belong to the same bin, say B_1 (observe that $v_2(b_{2^{n-1}}) = 1$); otherwise, $b_0, b_{2^{n-1}} \in B_1$, $b_{2^n} \in B_2$, say. If that is the case, then

$$\begin{aligned}
2^{N-1} &= \sum_{b_k \in B_1} b_k = b_0 + b_{2^{n-1}} + \sum_{\substack{k \neq 0, 2^{n-1} \\ b_k \in B_1}} b_k, \\
2^{N-1} &= \sum_{b_k \in B_2} b_k = b_{2^n} + \sum_{\substack{k \neq 2^n \\ b_k \in B_2}} b_k,
\end{aligned}$$

but that is impossible since both sums are now odd, but 2^{N-1} is even.

Assume now that $b_0, b_{2^{n-1}}, b_{2^n} \in B_1$. Further, we argue that, if $n \geq 4$, $b_{2^{n-2}}, b_{3 \cdot 2^{n-2}}$ also belong to B_1. We assume below the opposite.

Case 1. If $b_{2^{n-2}}, b_{3 \cdot 2^{n-2}}$ are split between B_1, B_2, then, without loss of generality (note that $b_{2^{n-2}} = b_{3 \cdot 2^{n-2}}$), we may assume

$$\begin{aligned}
2^{N-1} &= 2b_0 + b_{2^{n-2}} + b_{2^{n-1}} + \sum_{\substack{v_2(k) \neq 0, n, n-1 \\ b_k \in B_1}} b_k, \\
2^{N-1} &= b_{3 \cdot 2^{n-2}} + \sum_{\substack{v_2(k) \neq n-2 \\ b_k \in B_2}} b_k,
\end{aligned}$$

which implies that

$$v_2\left(\frac{1}{4}b_{3\cdot 2^{n-2}}+\frac{1}{4}\sum_{\substack{v_2(k)\neq n-2\\ b_k\in B_2}} b_k\right)=0\geq N-3\geq 1,\ \text{since } n\geq 4,$$

but this is impossible.
Case 2. If $b_{2^{n-2}}, b_{3\cdot 2^{n-2}}$ both belong to B_2, then

$$\begin{aligned} 2^{N-1}&=2b_0+b_{2^{n-1}}+\sum_{\substack{v_2(k)\neq 0,n,n-1\\ b_k\in B_1}} b_k,\\ 2^{N-1}&=2b_{2^{n-2}}+\sum_{\substack{v_2(k)\neq n-2\\ b_k\in B_2}} b_k. \end{aligned} \tag{10}$$

Applying [18, Theorem 1], we see that $b_{2^{n-1}}\equiv 6 \pmod{2^4}$, which implies that $v_2\left(2b_0+b_{2^{n-1}}\right)=3$, and since $N\geq 16$, then we must have $v_2\left(\sum_{\substack{v_2(k)\neq 0,n-1\\ b_k\in B_1}} b_k\right)=3$, and so, $b_{t\cdot 2^{n-3}}\in B_1$, for some odd t. Further, there exists also an odd t' such that $b_{t'\cdot 2^{n-3}}\in B_2$, because otherwise, $4\leq v_2\left(\sum_{\substack{v_2(k)\neq n-2\\ b_k\in B_2}} b_k\right)=v_2(2^{N-1}-2b_{2^{n-2}})=3$, an impossibility. Thus, B_1 must contain $b_{t\cdot 2^{n-3}}$, $t\in I_1^{(3)}\neq\emptyset$, and B_2 must contain $b_{t\cdot 2^{n-3}}$, $t\in I_2^{(3)}=\{1,3,5,7\}\setminus I_1^{(3)}\neq\emptyset$. Let $|I_1^{(3)}|=n_1, |I_2^{(3)}|=n_2=4-n_1$. Since $v_2\left(\sum_{t\in I_2^{(3)}} b_{t\cdot 2^{n-3}}+\sum_{\substack{v_2(k)\neq n-2,n-3\\ b_k\in B_2}} b_k\right)=v_2(2^{N-1}-2b_{2^{n-2}})=3$, we infer that $|I_1^{(3)}|, |I_2^{(3)}|\in\{1,3\}$. Next,

$$\begin{aligned} v_2\left(2^{N-1}-\sum_{\substack{v_2(k)\neq 0,n,n-1,n-3\\ b_k\in B_1}} b_k\right)&=v_2\left(2+b_{2^{n-1}}+\sum_{t\in I_1^{(3)}} b_{t\cdot 2^{n-3}}\right)\\ &=\begin{cases} 4 & \text{if } I_1^{(3)}=\{3,5,7\}, I_1^{(3)}=\{1,3,5\}, I_1^{(3)}=\{5\}, I_1^{(3)}=\{3\},\\ 6 & \text{if } I_1^{(3)}=\{7\}, I_1^{(3)}=\{1\},\\ 7 & \text{if } I_1^{(3)}=\{1,5,7\}, I_1^{(3)}=\{1,3,7\}. \end{cases} \end{aligned}$$

Further, since $I_2^{(3)}=\{1,3,5,7\}\setminus I_1^{(3)}$, then

$$\begin{aligned} v_2\left(2^{N-1}-\sum_{\substack{v_2(k)\neq n-2,n-3\\ b_k\in B_2}} b_k\right)&=v_2\left(2b_{2^{n-2}}+\sum_{t\in I_2^{(3)}} b_{t\cdot 2^{n-3}}\right)\\ &=\begin{cases} 4 & \text{if } I_2^{(3)}=\{1\}, I_2^{(3)}=\{7\}, I_2^{(3)}=\{1,3,7\}, I_2^{(3)}=\{1,5,7\},\\ 6 & \text{if } I_2^{(3)}=\{1,3,5\}, I_2^{(3)}=\{3,5,7\},\\ 7 & \text{if } I_2^{(3)}=\{3\}, I_2^{(3)}=\{5\}. \end{cases} \end{aligned}$$

Now, assuming $N \geq 6$, we argue modulo 2^5 in (10). Since $-2b_{2^{n-2}} \equiv 8 \pmod{2^5}$, then we must have $I_2^{(3)} \in \{\{1,3,5\},\{3,5,7\},\{3\},\{5\}\}$. For the complement $I_1^{(3)} = \bar{I}_2^{(3)}$, using [18], we compute the residues modulo 2^5 of the sum of binomial coefficients $b_{t\cdot 2^{n-3}}$, $t \in I_1^{(3)}$ and obtain that the residues are always 24 (mod 2^5), which does not equal the residue of $(2b_0 + b_{2^{n-1}}) \equiv 8 \pmod{2^5}$, obtaining a contradiction.

This argument will inductively work up to the $(n-1)$-st row of (9), where the 2-adic valuation of the b_k for every odd k attains its maximum n. We next assume that there are some b_{2k}, k odd, that belong to B_2, and so,

$$2^{N-1} = 2b_0 + b_{2^{n-1}} + (b_{2^{n-2}} + b_{3\cdot 2^{n-2}}) + \cdots + \sum_{\substack{v_2(k)=1 \\ b_k \in B_1}} b_k + \sum_{\substack{v_2(k)=0 \\ b_k \in B_1}} b_k$$

$$2^{N-1} = \sum_{\substack{v_2(k)=1 \\ b_k \in B_2}} b_k + \sum_{\substack{v_2(k)=0 \\ b_k \in B_2}} b_k.$$

Label $A := \sum_{\substack{v_2(k)=1 \\ b_k \in B_1}} b_k$, $B := \sum_{\substack{v_2(k)=0 \\ b_k \in B_1}} b_k$. It is known [21, Theorem 3] that the sum of all binomial coefficients on the k-th row of (9) has the 2-adic valuation equal to $2^k - 1$, that is, for

$$R_k := \sum_{t=0}^{2^{k-1}-1} \binom{2^n}{(2t+1)2^{n-k}}, \quad v_2(R_k) = 2^k - 1. \tag{11}$$

From (11), we know that $v_2(R_k) = 2^k - 1$. It is also not difficult to find that $R_n = 2^{2^n-1}$ and $R_{n-1} = 2^{2^{n-1}-1}\left(2^{2^{n-1}-1} - 1\right)$. Observe that

$$\sum_{\substack{v_2(k)=1 \\ b_k \in B_2}} b_k = R_{n-1} - \sum_{\substack{v_2(k)=1 \\ b_k \in B_1}} b_k = R_{n-1} - A, \text{ and}$$

$$\sum_{\substack{v_2(k)=0 \\ b_k \in B_2}} b_k = R_n - \sum_{\substack{v_2(k)=1 \\ b_k \in B_1}} b_k = 2^{N-1} - B.$$

We therefore get

$$2^{2^n-1} = 2b_0 + b_{2^{n-1}} + \sum_{k=2}^{n-2} R_k + A + B$$

$$2^{2^{n-1}-1}\left(2^{2^{n-1}-1} - 1\right) = A + B. \tag{12}$$

While we conjecture that there are only two bisections for n even and 6 bisections for n odd (supported by the included data), we are unable to show that. Instead, we find an upper bound for J_{2^n}, which is better than the one given by Theorem 5.

We now use Freiman's Theorem 2, with $M := 2^{n-1} + 2^{n-2} = 3 \cdot 2^{n-2}$ variables (this is the number of binomial coefficients $\binom{2^n}{k}$), where $v_2(k) = 0, 1$), $b := R_{n-1} = 2^{2^{n-1}-1}\left(2^{2^{n-1}-1} - 1\right)$, $a_j = \binom{2^n}{2(2j-1)}$, $1 \leq j \leq 2^{n-2}$, and $a_j = \binom{2^n}{2(j-2^{n-2})-1)}$, $2^{n-2}+1 \leq j \leq 2^{n-2}+2^{n-1}$, to obtain that the number of ways of solutions for the equation (12) is (we shall use again Hölder inequality, as well as $a_j = a_{2^n-j}$ below; also, set $b_j := a_j, 1 \leq j \leq 2^{n-3}, b_j := a_{j+2^{n-3}}, 2^{n-3}+1 \leq$

$j \le 2^{n-2}+2^{n-3}$)

$$
\begin{aligned}
J_b &= \int_0^1 e^{-2\pi i x b}\prod_{j=1}^{M}(1+e^{2\pi i x a_j})d\,x = \int_0^1 e^{-2\pi i x b}\prod_{j=1}^{M}\left(2\cos(\pi i x a_j)e^{\pi i x a_j}\right)d\,x \\
&= 2^M\int_0^1 e^{-2\pi i x b}\prod_{j=1}^{M}\cos(\pi i x a_j)e^{\sum_{j=1}^{M}\pi i x a_j}d\,x \\
&= 2^M\int_0^1 e^{-2\pi i x b}\prod_{j=1}^{M}\cos(\pi i x a_j)e^{\pi i x(R_{n-1}+R_n)}d\,x \\
&= 2^M\int_0^1 e^{-2\pi i x b}\prod_{j=1}^{M}\cos(\pi i x a_j)e^{\pi i x(b+2^{2^n-1})}d\,x \\
&= 2^M\int_0^1 e^{\pi i x(2^{2^n-1}-b)}\prod_{j=1}^{M/2}\cos^2(\pi i x b_j)d\,x \\
&\le 2^M\left(\prod_{j=1}^{M/2}\int_0^1\cos^M(\pi x b_j)\right)^{2/M} = 2^M\frac{1}{2^M}\binom{M}{M/2} \\
&\sim \frac{2^M}{\sqrt{\pi M/2}} \sim 0.3258\cdot 2^{3\cdot 2^{n-2}-2^{\frac{n-3}{2}}},
\end{aligned}
$$

and the theorem is shown. □

Conjecture 8. *We conjecture that* $J_{2^n} = \begin{cases} 2 & \text{if } n \text{ even} \\ 6 & \text{if } n \text{ odd} \end{cases}$.

4 Some computational results and exact counts

Using the Hamming High Performance Computer (HPC) at the Naval Postgraduate School, and a parallel computer program written in Julia, we were able to verify the computational data of [7, 19] and obtain additional results for the number of bisections J_n, for $n \le 51$ (for n odd we write the number of bisections as $2^{(n+1)/2}+\cdots$ to point out how many are nontrivial), displayed in Table 1.

A portion of this sequence, for $n \le 36$, appears as A200147 in the OEIS (Online Encyclopedia of Integer Sequences), as the number x_n, $n \ge 1$, of 0 or 1 arrays, $[a_0, a_1, ..., a_n]$, of $n+1$ elements, with zero n-difference. In general, given a sequence $\{a_n\}_{n\ge 1}$ of real or complex numbers, the *first difference sequence* $\Delta(a_n)$ is defined as $\Delta(a_n) = a_{n+1} - a_n$ for all $n \ge 1$. If we just have a list $L = [a_0, a_1, ..., a_n]$, then the *first difference of* L, $\Delta(L)$, is simply the list $\Delta(L) = [a_1 - a_0, a_2 - a_1, ..., a_n - a_{n-1}]$ which has only n-items. The second difference $\Delta^2(a_n)$ is defined as $\Delta^2(a_n) = \Delta(a_{n+1}) - \Delta(a_n)$, and we have similar definitions for lists. To establish the correspondence between the two countings, let us observe that

$$\Delta^k(a_n) = \Delta^{k-1}(a_{n+1}) - \Delta^{k-1}(a_n) = \sum_{t=0}^{k}\binom{k}{t}(-1)^t a_{n+k-t}. \tag{13}$$

Table 1: Number of Binomial Coefficients Bisections

n	J_n	n	J_n	n	J_n
1	2	18	2	35	$2^{18}+24$
2	2	19	2^{10}	36	2
3	2^2	20	6	37	2^{19}
4	2	21	2^{11}	38	38
5	2^3	22	2	39	2^{20}
6	2	23	2^{12}	40	2
7	2^4	24	50	41	$2^{21}+15\cdot 2^{11}$
8	6	25	2^{13}	42	2
9	2^5	26	6	43	2^{22}
10	2	27	2^{14}	44	134
11	2^6	28	2	45	2^{23}
12	2	29	$2^{15}+2^{11}$	46	2
13	2^7+2^4	30	2	47	$2^{24}+2^{20}$
14	14	31	$2^{16}+5\cdot 2^7$	48	4098
15	2^8	32	6	49	2^{25}
16	2	33	$2^{17}+2^{14}$	50	6
17	2^9	34	130	51	2^{26}

From what we have seen, if $n=8$, $L:=[1,-1,-1,1,1,-1,-1,-1,1]$ is a nontrivial solution for (BCB) problem. By (13), the list

$$L=[1,1,-1,-1,1,1,-1,1,1]$$

is a solution of $\Delta^8(L)=[0]$ (by alternating signs). Adding a constant to a sequence does not change its differences Δ^k, and multiplying a sequence by a number, it is just a multiplicative factor for all the differences. Hence, the list

$$\widetilde{L}=(L+1)/2=[1,1,0,0,1,1,0,1,1] \tag{14}$$

is a 0 or 1 array of 9 elements with a zero 8-difference:

$$\Delta(\widetilde{L})=[0,-1,0,1,0,-1,1,0],\ \Delta^2(\widetilde{L})=[-1,1,1,-1,-1,2,-1],$$

$\Delta^3(\widetilde{L})=[2,0,-2,0,3,-3]$, $\Delta^4(\widetilde{L})=[-2,-2,2,3,-6]$, $\Delta^5(\widetilde{L})=[0,4,1,-9]$, $\Delta^6(\widetilde{L})=[4,-3,-10]$, $\Delta^7(\widetilde{L})=[-7,-7]$, and finally $\Delta^8(\widetilde{L})=[0]$.

The formulas (13) and (14) give essentially the bijection between the set of solutions of (BCB) problem and the arrays described in the sequence A200147. Let us record this observation and fill in the details.

Proposition 9. *The number of bisections of the binomial coefficients, J_n, is the same as the number of 0's or 1's arrays, of $n+1$ elements, with zero n-difference, i.e., $J_n=x_n$.*

Proof. Suppose we have a solution $L := [\delta_0, \ldots, \delta_n]$ of the (BCB) problem. Hence, $\sum_{i=0}^{n} \delta_i \binom{n}{i} = 0$, $\delta_i \in \{-1, 1\}$. From (13), we see that this is equivalent to $\Delta^n(\widehat{L}) = 0$ where $\widehat{L} = [\delta_0, -\delta_1, \ldots, (-1)^n \delta_n]$. As we have observed in the Introduction, adding a constant to $\widehat{L}$, does not affect the differences Δ^k, i.e., we still have $\Delta^n(\widehat{L} + 1) = 0$. Finally, since

$$\widehat{L} + 1 = [1 + \delta_0, 1 - \delta_1, \ldots, 1 + (-1)^n \delta_n]$$

is a list of 2's or 0's we can divide by 2 to obtain an array of 0's or 1's: $\widetilde{L} = [(1 + \delta_0)/2, (1 - \delta_1)/2, \ldots, (1 + (-1)^n \delta_n)/2]$ for which we still have $\Delta^n(\widetilde{L}) = \Delta^n(\widehat{L})/2 = 0$. It is clear that the map

$$L \to \widetilde{L} = \frac{1}{2}(\widehat{L} + 1)$$

establishes a bijection between the sets in discussion. □

We say that f is SAC [29] if complementing any one of the n input bits the output changes with probability exactly one half. A Boolean function of n variables satisfies the SAC of order k (we say f is $SAC(k)$ – see [10]), $0 \leq k \leq n-2$, if whenever k input bits are fixed, the resulting function of $n - k$ variables satisfies the SAC.

In what follows we will show that $J_n = 2$ for infinitely many values of n, which will imply conjecture $Q2$ of Cusick and Li [7], hence $Q4$, as well, and so, there are only four symmetric $SAC(k)$ functions for infinitely many n.

First, we let $v_2(n)$ be the 2-adic valuation of n, that is, the largest power of 2 occurring in the prime power factorization of n (we write $2^{v_2(n)} || n$) (we slightly abuse the notation, as it is usually customary to define the 2-adic valuation as $2^{-v_2(n)}$).

Theorem 10. *If p is a prime number, then $J_{p-1} = 2$.*

Proof. The statement is obviously true if $p = 2$, so we may assume that p is an odd prime. We let $n = p - 1$ and observe that $n \equiv -1 \pmod{p}$. We want to show that $\binom{n}{j} \equiv (-1)^j \pmod{p}$, for every $j \in \{0, 1, \ldots, n\}$. This is clearly true for $j = 0$. Since, every $j \in \{1, \ldots, n\}$ has an inverse modulo p, we have for $j \in \{1, \ldots, n\}$

$$\begin{aligned} \binom{n}{j} &\equiv \frac{n(n-1)\cdots(n-j+1)}{j!} \\ &\equiv \frac{(-1)(-2)\cdots(-1-j+1)}{j!} \equiv (-1)^j \pmod{p}. \end{aligned}$$

Hence, if $[\delta_0, \ldots, \delta_n]$ a solution of the (BCB) problem

$$0 = \sum_{j=0}^{n} \delta_j \binom{n}{j} \equiv \sum_{j=0}^{n} (-1)^j \delta_j \pmod{p}.$$

But the number

$$\Delta := \sum_{j=0}^{n} (-1)^j \delta_j \equiv 0 \pmod{p}$$

is an odd number ($n + 1 = p$ is an odd prime) satisfying

$$|\Delta| \leq \sum_{j=0}^{n} |(-1)^j \delta_j| = \sum_{j=0}^{n} 1 = n+1 = p. \tag{15}$$

Because Δ cannot be zero, the only possible values of Δ are p or $-p$. Then the equality $|\Delta| = p = n+1$ in (15), forces $\delta_j = \pm(-1)^j$, for all j. Therefore, we have only the two trivial solutions, that is, $J_n = 2$. □

Next, we are going to use the following construction of a transformation on solutions of the (BCB), denoted here by Θ, which we are going to call *backward map*. Let $n \in \mathbb{N}$ with $n \geq 2$ and $\delta = [\delta_0, \ldots, \delta_n]$ be a solution of the (BCB) problem. Hence $\sum_{i=0}^{n} \delta_i \binom{n}{i} = 0$ with $\delta_i \in \{-1, 1\}$. Using the Pascal binomial identity

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

we have $\delta_0 + \delta_n + \sum_{i=1}^{n-1} \delta_i \left(\binom{n-1}{i} + \binom{n-1}{i-1} \right) = 0$. Rearranging terms, we obtain

$$\delta_0 + \delta_1 + \sum_{i=1}^{n-1} (\delta_i + \delta_{i+1}) \binom{n-1}{i} = 0.$$

If we define $\eta_j = (\delta_j + \delta_{j+1})/2$, $j \in \{0, 1, ..., n-1\}$, the identity above becomes $\sum_{i=0}^{n-1} \eta_i \binom{n-1}{i} = 0$. Let us denote the map $[\delta_0, \ldots, \delta_n] \to [\eta_0, \eta_1, \ldots, \eta_{n-1}]$ by Θ. If we restrict the domain of this map to solutions for which $\delta_0 = 1$ then it becomes a one-to-one map. We observe that $\eta_j \in \{-1, 0, 1\}$ for all j. So, if we have a trivial solution δ we get $\Theta(\delta) = 0$. Given a sequence $\eta = [\eta_0, \eta_1, \ldots, \eta_{n-1}] = \Theta(\delta)$ for some δ, we see that $\eta_j = 1$ forces $\delta_j = 1$ and $\delta_{j+1} = 1$. Similarly, if $\eta_j = -1$, forces $\delta_j = -1$ and $\delta_{j+1} = -1$. Hence we cannot have two consecutive η's having a change of signs, i.e., it must go through a zero value. In fact, the number of zero's between two changes of sign should be odd. Let us call this property the *(IVP) property* since it resembles the Intermediate Value Property in Calculus. It is easy to see that a sequence like that is then in the range of Θ. Having a non trivial solution $\delta' \in \mathcal{J}_{n-1}$, this leads to two identities η_1 and η_2. If one of these vectors has the (IVP) we say that δ' has the (IVP). Let us observe that identities like $\binom{n}{k} - \binom{n}{n-k} = 0$ have (IVP), if and only if n is even.

Corollary 11. *If p is an odd prime, then $\mathcal{J}_{p-2}$ cannot contain nontrivial solutions which have the (IVP) property.*

Proof. If by way of contradiction, we have a nontrivial solution δ' which has (IVP), then it leads to a nonzero identity η which can be lifted up to $\delta \in \mathcal{J}_{p-1}$, i.e. $\eta = \Theta(\delta)$. But we have shown that the only solutions in $\mathcal{J}_{p-1}$ are the trivial ones. Hence, $\eta = \Theta(\delta) = 0$ and so we get into a contradiction. □

This suggests that the only solutions that we can have in $\mathcal{J}_{p-2}$ are the ones that lead to trivial identities of the form $\binom{n}{k} - \binom{n}{n-k} = 0$ or sums of these (which cannot be lifted since $p-2$ is odd). This explains why, numerically, $J_{p-2} = 2^{\frac{p-1}{2}}$ for many primes p.

The Julia program we use represents bisection solutions it finds as binary vectors, $\overrightarrow{v_n}$ (see the appendix). Given the n^{th} row of Pascal's triangle, $\overrightarrow{p_n}$, along with a corresponding bisection, we represent the dot product as: $\overrightarrow{p_n} \cdot \overrightarrow{v_n} = 2^{n-1}$. By inspecting the nontrivial solution vectors we observe the fact that the pattern 10011001 occurs in the nontrivial bisection for $n = 13$ and so, prompted by that, we search for other cases where we can insert 1001 at position $n - k$ in the first half, as well as in the corresponding position in the second half.

Looking at the bisection solution data (see the appendix) we see some other patterns showing up. We will first consider some identities that were pointed out by Jefferies [19], and find the complete solutions set for the implied diophantine equations, rendering, yet again other infinite classes of integers admitting nontrivial bisections.

Theorem 12. *We have:*

1. *If $n = k^2 - 2$, $k \geq 4$ even, then $J_n \geq 10$, $J_{n-1} \geq 2^{\frac{n+1}{2}} + 2^{\frac{n+1}{2}-3}$ (tight).*
2. *If $k \equiv 0, 1 \pmod 3$ and $n = \frac{F_{4k+1}+2F_{4k}-6}{5}$, then $J_n \geq 2^{\frac{n+1}{2}} + 2^{\frac{n-3}{2}}$.*
3. *Let $n = 4k^2 + 16k + 13, k \geq 0$. Then, there are at least $2^{(n+1)/2-3}$ nontrivial bisections for the binomial coefficients $\left\{\binom{n}{j}\right\}_{0 \leq j \leq n}$, and so, $J_n \geq 2^{\frac{n+1}{2}} + 2^{\frac{n-1}{2}}$.*

Proof. We first consider the identity

$$\binom{n}{x} + \binom{n}{x+2} = 2\binom{n}{x+1}. \tag{16}$$

By expanding and canceling out the factorials, we obtain the diophantine equation (assume that $n > 1$)

$$n^2 - 4nx + 4x^2 - 5n + 8x + 2 = 0.$$

We will take an elementary approach to this equation, and write it as

$$(n - 2x)^2 - 4(n - 2x) - n + 2 = (n - 2x - 2)^2 - n - 2 = 0,$$

that is, $n - 2x - 2 = \pm k$ and $n + 2 = k^2$, $k \in \mathbb{Z}$, and so, we get the integer solutions for (16)

$$n = k^2 - 2, \quad x = \frac{k^2 \mp k}{2} - 2.$$

Note that Jefferies [19] provides only the even solutions.

Now, we must argue whether these identities will generate nontrivial bisections. As we mentioned previously, the way we use these identities is to transform a trivial bisection into nontrivial ones by interchanging the two sides of the identity, assuming each side occurs in the same bisection. If n odd, recall that a trivial bisection is obtained by taking randomly the first half of the coefficient $\{0, 1\}$-vector, and the second half is the complement. However, in our case, these binomials occur in the first half, so this identity will not give us nontrivial bisections. If n is even, we get the two trivial bisections by putting all even indexed binomials in one bin, and all the odd indexed ones in the other bin. Since $x \equiv x+2 \not\equiv x+1 \equiv n-(x+1) \pmod 2$, then this identity will give us eight more (four such for each choice of the $\mp$ sign) nontrivial bisections (see also [19]).

We now look at the binomial identity, which while observed in [19] for $n = 13, x = 3$, or $x = 7$, was not solved there in its full generality:

$$\binom{n}{x} + \binom{n}{x+3} = \binom{n}{x+1} + \binom{n}{x+2}. \tag{17}$$

Equation (17) is equivalent to

$$n^2 + 4x^2 - 4nx - 7n + 12x + 6 = 0.$$

It turns out that it is as easy as the previous diophantine equation and a similar elementary approach renders the solutions

$$n = k^2 - 3, \quad x = \frac{k^2 \mp k}{2} - 3.$$

In the case of odd n, the situation is different. The idea is to transform a trivial bisection (whose second half $\{0,1\}$-vector is the complement of the arbitrarily chosen first half) by keeping a small vector fixed in the first half (and the second half), which we show that has equal sum. For the previous values of n, x, we obtain $2 \cdot 2^{\frac{n+1}{2}-4}$ many nontrivial bisections (a tight bound as we see from our table, since $J_{13} = 2^{\frac{13+1}{2}} + 2^4$).

Next, we consider the binomial equation

$$\binom{n}{x+2} = \binom{n}{x+1} + \binom{n}{x}. \tag{18}$$

We point out that the single solution $(n, x) = (117, 38)$ provided in [19] is incorrect, and it should rather be $(n, x) = (103, 38)$. In fact, we shall find all solutions to this diophantine equation, although, the method is slightly more complicated than the previous diophantine equations. We do not claim that this equation has not been considered before, but we were not able to find a suitable reference.

From (18) we obtain

$$n^2 + x^2 - 3nx - 3n - 2 = 0,$$

which can be written (multiplying by 20 so that we have an equation in integers) as the Pell equation (for convenience, we take $x \leq n/2$, so $3n > 2x$)

$$(5n + 6)^2 - 5(3n - 2x)^2 = -4. \tag{19}$$

Our reason for purposefully disregarding a (well-known to specialists) recurrence identity (namely, $L_n^2 - 5F_n^2 = 4(-1)^n$, where F_n, L_n are the Fibonacci, respectively Lucas numbers, satisfying the same recurrence $F_{m+1} = F_m + F_{m-1}$, with $F_0 = 0, F_1 = 1$, $L_0 = 2, L_1 = 1$) is two-fold: it is not obvious that the mentioned identity will render *all* solutions to our diophantine equation; secondly, we wish to give yet another proof to that identity via Pell equations theory.

Fortunately, the Pell equation $X^2 - 5Y^2 = -4$ can be solved precisely in a form that is convenient to us (see [22, 28]). First, observe that $(x_1, y_1) = (1, 1)$ is its fundamental solution. Pell equation theory shows that all solutions to $X^2 - 5Y^2 = -4$ are then (x_{2n+1}, y_{2n+1}), where

$$x_{2m+1} + y_{2m+1}\sqrt{5} = \frac{1}{2^{2m}}(1 + \sqrt{5})^{2m+1} = 2\phi^{2m+1},$$

where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden mean. We now use the identity

$$\phi^k = \phi F_k + F_{k-1},$$

therefore,

$$(x_{2m+1}, y_{2m+1}) = (F_{2m+1} + 2F_{2m}, F_{2m+1}),$$

are all solutions to $X^2 - 5Y^2 = -4$, and so, the following solutions for (19)

$$n = \frac{F_{2m+1} + 2F_{2m} - 6}{5},$$
$$x = \frac{3F_{2m} - F_{2m+1} - 9}{5},$$

assuming they are integers. It is rather easy to show that m must be even, say $m = 2k$ and so, the general solution to (18) now becomes

$$n = \frac{F_{4k+1} + 2F_{4k} - 6}{5},$$
$$x = \frac{4F_{4k+1} + 3F_{4k} - 9}{5}.$$

We are looking for odd values of n, which will happen if F_{4k+1} is odd. Using the entry point modulo 2 for the Fibonacci numbers, we infer that F_{4k+1} is odd if $k \equiv 0, 1 \pmod 3$.

Certainly, since then for such an odd n we could "destroy" the triviality of a bisection by placing, for $x < n/2$, the binomials $\binom{n}{x}, \binom{n}{x+1}$ in one bin and $\binom{n}{x+2}$ in another bin (similarly, for $x > n/2$), we infer that there are more than $2 \cdot 2^{\frac{n+1}{2}-3}$ nontrivial bisections in this case.

Next, we define the operation $\tilde{\cdot}$ on a $\{0,1\}$-bit block B, which outputs the mirror image block $\tilde{B}$. For example, $\widetilde{100} = 001$. Also, recall that $\bar{B}$ is the complement of the block B.

Let $n = 2t + 1$ and k to be determined later. The idea is to start with a trivial bisection $H||\bar{\tilde{H}}$ (where H is a random first block) for n and replace a 4-bit block k bits away from the middle of the sequence) in H and the corresponding 4-bit block in $\bar{\tilde{H}}$ by $1001\overbrace{\cdots}^{k}||\overbrace{\cdots}^{k}1001$ (similarly, by $0110\overbrace{\cdots}^{k}||\overbrace{\cdots}^{k}0110$) to preserve the bisection.

Here, we force n to satisfy the following binomial coefficient identity

$$\begin{aligned}&\binom{n}{t-k-3} + \binom{n}{t-k} + \binom{n}{t+k+1} + \binom{n}{t+k+4}\\ =&\binom{n}{t-k-1} + \binom{n}{t-k-2} + \binom{n}{t+k+2} + \binom{n}{t+k+3},\end{aligned}$$

which is equivalent to

$$\binom{n}{t-k-3} + \binom{n}{t-k} = \binom{n}{t-k-1} + \binom{n}{t-k-2}.$$

Multiplying the above equation by $\frac{(t-k-3)!(t+k+1)!}{n!}$ we obtain the equation

$$\frac{1}{(t+k+2)(t+k+3)(t+k+4)} + \frac{1}{(t-k)(t-k-1)(t-k-2)}$$

$$= \frac{1}{(t-k-1)(t-k-2)(t+k+2)} + \frac{1}{(t-k-2)(t+k+2)(t+k+3)},$$

which renders the diophantine equation

$$6 + 8k + 2k^2 - t = 0,$$

therefore, for every value of $k \geq 0$, one can take $n = 2t+1 = 4k^2+16k+13$, for which there are (at least two) nontrivial bisections. The bound can be improved observing that the first $(n+1)/2 - 4$ bits can be taken arbitrarily. □

5 Appendix

We display below the values of $n \leq 10000$ given by Theorem 12, for which there are nontrivial bisections, namely,

$$13, 14, 33, 34, 61, 62, 97, 98, 103, 141, 142, 193, 194, 253, 254, 321, 322,$$
$$397, 398, 481, 482, 573, 574, 673, 674, 713, 781, 782, 897, 898, 1021, 1022,$$
$$1153, 1154, 1293, 1294, 1441, 1442, 1597, 1598, 1761, 1762, 1933, 1934,$$
$$2113, 2114, 2301, 2302, 2497, 2498, 2701, 2702, 2913, 2914, 3133, 3134,$$
$$3361, 3362, 3597, 3598, 3841, 3842, 4093, 4094, 4353, 4354, 4621, 4622,$$
$$4897, 4898, 5181, 5182, 5473, 5474, 5773, 5774, 6081, 6082, 6397, 6398,$$
$$6721, 6722, 7053, 7054, 7393, 7394, 7741, 7742, 8097, 8098, 8461, 8462,$$
$$8833, 8834, 9213, 9214, 9601, 9602, 9997, 9998.$$

The table which follows contains the complete set of nontrivial bisection solution vectors for $1 \leq n \leq 50$. In the interest of saving space, we only list the highest lexicographically occurring solutions. Any additional solutions which a listed solution may yield, can be generated in the following manner: If a pair of bits are equidistant from the center of the given vector and differ, they may both be complemented to produce a new solution. Additionally, any solution vector can also be reversed and complemented in its entirety to produce yet another solution.

n	# nontrivial sols.	nontrivial sol. vectors
8	4	100110001
13	16	11110011001000
14	4	101001101000101
	8	101011100100101
20	4	101010011010100010101
24	32	100011011011000100010001
	16	101100111101010010100 0101
26	4	10101010011010101000101 0101
29	2048	11111111011101100011001000 0000
31	512	11110110011111100010101000001000
	128	11110110010110011001100000001000
32	4	10101010100110101010100010101 0101
33	16384	11111111111110011010010000000000
34	64	10101001110110111010000000110010101
	32	10101001110111101010010000110010101
	16	10101001111100111010000110110010101
	8	10101001111101101010010110110010101
	8	10101010101011011010001010101010101
35	8	10101010101010011100100101010101010101
	16	10101010101110011100100011010101010101
38	4	10101010101001101010101010010010101010101
	32	10111111001011111010001110001001101 1101
41	2048	11111101111010100111100010010000111010000 0
	4096	11111101111011100111100010001000111010000 0
	8192	11111111111100101011100100010010001010000 0
	16384	11111111111101101011100100001010001010000 0
44	4	10101010101010011010101010101000101010101 0101
	128	10101111100011111111011000001101100011011 0101
47	1048576	11111111111111010011111100000100000100000000000
48	4096	10110011110110110101110101010000000000001000000101
50	4	10101010101010100110101010101010100010101010101 0101

References

[1] D. Andrica, E.J. Ionascu, *Some Unexpected Connections Between Analysis and Combinatorics*, In Mathematics Without Boundaries, Surveys in Pure Mathematics, pages 1–19, Springer-Verlag, 2014.

[2] L. Baker, S. Wagner, *Erdös-Surányi sequences and trigonometric integrals*, arXiv:1506.04555, 2015.

[3] N.M. Blachman, Noise and its effect on communication, New York, London: McGraw-Hill, 1966.

[4] P.L. Buzytsky, *An effective formula for the number of solutions of linear Boolean equations*, SIAM J. Alg. Disc. Meth. 3:2 (1982), 182–186.

[5] M. Chaimovich, G. Freiman, Z. Galil, *Solving dense subset-sum problems by using analytical number theory*, J. Complexity 5 (1989), 271–282.

[6] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.-P. Schnorr, J. Stern, *Improved low-density subset sum algorithms*, Comput. Complexity 2 (1992), 111–128.

[7] T.W. Cusick, Y. Li, *k-th order symmetric SAC boolean functions and bisecting binomial coefficients*, Discrete Appl. Math. 149 (2005), 73–86.

[8] M.O. Drimbe, *Generalization of representation theorem of Erdös and Surányi*, Comment. Math. Prace Mat. 27:2 (1988), 233–235.

[9] J.D. Farmer, S.C. Leth, *An Asymptotic Formula for Powers of Binomial Coefficients*, Math. Gazette 89:516 (2005), 385–391.

[10] R. Forré, *The strict avalanche criterion: spectral properties of Boolean functions and an extended definition*, Adv. in Cryptology – Crypto. '88, pp. 450–468.

[11] G.A. Freiman, *An analytical method of analysis of linear Boolean equations*, Ann. N.Y. Acad. Sci. 337 (1980), 97–102.

[12] G.A. Freiman, *On Solvability of a System of Two Boolean Linear Equations*, Number Theory: New York Seminar 1991–1995, 135–150.

[13] M.R. Garey, D.S. Johnson, Computer and Intractability: A Guide to the Theory of NP-Completeness, W.H. Freeman and CO., San Francisco, 1979.

[14] J. von zur Gathen, J. Roche, *Polynomials with two values*, Combinatorica 17 (1997), 345–362.

[15] P. Goetgheluck, *Computing binomial coefficients*, American Math. Monthly 94:4 (1987), 360–365.

[16] K. Gopalakrishnan, D.G. Hoffman, D.R. Stinson, *A note on a conjecture concerning symmetric resilient functions*, Inform. Proc. Lett. 47 (1993), 139–143.

[17] R.L. Graham, D.E. Knuth, O. Patashnik, Concrete Mathematics: A Foundation for Computer Science, 2nd edition, 1994.

[18] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, in Organic mathematics (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.

[19] N. Jefferies, *Sporadic partitions of binomial coefficients*, Elec. Lett. 27:15 (1991), 134–136.

[20] J.C. Lagarias, A.M. Odlyzko, *Solving Low-Lensity Subset Sum Problems*, J. Assoc. Comp. Mach. 32:1 (1985), 229–246.

[21] T. Lengyel, *On the order of lacunary sums of binomial coefficients*, Integers: Electronic J. Combin. Number Theory 3 (2003), #A03.

[22] K. Matthews, *The Diophantine Equation* $x^2 - Dy^2 = N$, $D > 0$, Expositiones Math. 18 (2000), 323–331.

[23] R. Merkle, M. Hellman, *Hiding Information and Signatures in Trapdoor Knapsacks*, IEEE Trans. Inf. Theory 24:5 (1978), 525–530.

[24] C. Mitchell, *Enumerating Boolean functions of cryptographic significance*, J. Cryptology 2 (1990), 155–170.

[25] G. Polya, G. Szegö, Problems and Theorems in Analysis I: Series, Integral Calculus, Theory of Functions, 1972.

[26] P. Stănică, *Good Lower and Upper Bounds on Binomial Coefficients*, J. Inequalities in Pure and Applied Math., Vol.2, Issue 3 (2001), Art. 30.

[27] J. Rogawski, Calculus, W. H. Freeman and Company, 2008.

[28] A. Tekcan, *The Pell Equation* $x^2 - Dy^2 = \pm 4$, Appl. Math. Sciences 1:8 (2007), 363–369.

[29] A.F. Webster, S.E. Tavares, *On the design of S-boxes*, Advances in Cryptology – Crypto. 1985, pp. 523–534.