Taylor & Francis
Taylor & Francis Group

Mathematics Magazine

ISSN: 0025-570X (Print) 1930-0980 (Online) Journal homepage: https://www.tandfonline.com/loi/umma20

Boolean Function Analogs of Covering Systems

Anthony Zaleski & Doron Zeilberger

To cite this article: Anthony Zaleski & Doron Zeilberger (2020) Boolean Function Analogs of Covering Systems, Mathematics Magazine, 93:1, 54-61, DOI: 10.1080/0025570X.2020.1684797

To link to this article: https://doi.org/10.1080/0025570X.2020.1684797

Published online: 22 Jan 2020.

Boolean Function Analogs of Covering Systems

ANTHONY ZALESKI
Rutgers University
New Brunswick, NJ 08901
anthony.zaleski@rutgers.edu

DORON ZEILBERGER
Rutgers University
New Brunswick, NJ 08901
doronzeil@gmail.com

Abstraction is a great tool for mathematicians. Often, a problem that at first seems intimidating is suddenly endowed with an elegant solution, once it is embedded in a more general space. Like misdirection in a magic trick, certain specifics can blind one to the bigger picture; they are conceptual red herrings.

For example, the French mathematical columnist Jean-Paul Delahaye [4] recently posed the following brain-teaser, adapting a beautiful puzzle, of unknown origin, popularized by Peter Winkler [9, pp. 35–43].

Here is a free translation from the French:

Enigma: nine beetles and prime numbers

One places nine beetles on a circular track in such a way that the nine arc distances, measured in meters, between two consecutive beetles are the first nine prime numbers, 2, 3, 5, 7, 11, 13, 17, 19, and 23. The order is arbitrary, and each number appears exactly once as a distance.

At starting time, each beetle decides *randomly* whether she would go, traveling at a speed of 1 meter per minute, clockwise or counter-clockwise. When two beetles bump into each other, they immediately do a “U-turn,” i.e., reverse direction. We assume that the size of the beetles is negligible. At the end of 50 minutes, after many collisions, one notices the distances between the new positions of the beetles. The nine distances are exactly as before, the first nine prime numbers! How to explain this miracle?

Before going on to the next section, we invite you to solve this puzzle all by yourself.

Solution of the enigma Note that the length of the circular track is

$$2+3+5+7+11+13+17+19+23=100$$

meters.

Let each beetle carry a flag, and whenever two beetles bump into each other, let them exchange flags. Since the flags always move in the same direction, and also move at a speed of 1 meter per minute, after 50 minutes, each flag is *exactly* at the antipode of its original location; hence, the distances are the same! Of course, this works if the original distances were *any* sequence of numbers: All that they have to obey is that their sum equals 100, or more generally, that half the sum of the distances divides the product of the speed (1 meter per minute in this puzzle) and the elapsed time (50 minutes in this puzzle).

Math. Mag. **93** (2020) 54–61. doi:10.1080/0025570X.2019.1684797 © Mathematical Association of America
MSC: 03B35, 05A99

This variation, due to Delahaye, is *much* harder than the original version posed by Winkler [9], where also the initial distances were arbitrary. In Delahaye's rendition, the solver is bluffed into trying to use the fact that the distances are primes; this was the red herring. Something analogous happened to Paul Erdős, concerning *covering systems*.

Covering systems

In 1950, Paul Erdős introduced the notion of *covering systems* [5]. A covering system is a finite set of arithmetical progressions

$$\{a_i \pmod{m_i} \quad | \quad 1 \leq i \leq N\},$$

whose union is the set of all non-negative integers. For example

$$\{0 \pmod{1}\},$$

is such a (not very interesting) covering system, while

$$\{0 \pmod{2}\ ,\ 1 \pmod{2}\},$$

and

$$\{0 \pmod{5},\ 1 \pmod{5},\ 2 \pmod{5},\ 3 \pmod{5},\ 4 \pmod{5}\},$$

are other, almost as boring, examples. A slightly more interesting example is

$$\{0 \pmod{2},\ 1 \pmod{4},\ 3 \pmod{4}\}.$$

A covering system is *exact* if all the congruences are disjoint (like in the above boring examples). It is *distinct* if all the moduli are different. (From now on, let $a\ (b)$ mean $a \pmod{b}$.)

Erdős [6] gave the smallest possible example of a distinct covering system:

$$\{0\,(2),\ 0\,(3),\ 1\,(4),\ 5\,(6),\ 7\,(12)\}.$$

Of course, the above covering system is not exact since, for example, 0 (2) and 0 (3) both contain any multiple of 6. A theorem proved by Mirsky and (Donald) Newman, and independently by Davenport and Rado (described by Erdős [6]) implies that a covering system cannot be both exact *and* distinct. Even a stronger statement holds. Assuming that our system $\{a_i(m_i)\}_{i=1}^{N}$ is written in non-decreasing order of the moduli $m_1 \leq m_2 \leq \cdots \leq m_N$, the Mirsky–Newman–Davenport–Rado theorem asserts that $m_{N-1} = m_N$. In other words, the two top moduli are equal (and hence an exact covering system can never be distinct). See Zeilberger [10] for an exposition of their snappy proof. While their proof was nice, it was not as nice as the combinatorial-geometrical proof that was found by Berger, Felzenbaum, and Fraenkel [1, 2], and exposited by Zeilberger [10]. In fact, they proved the more general Znam theorem that asserts that the highest modulus shows up at least p times, where p is the smallest prime dividing $\operatorname{lcm}(m_1, \ldots, m_N)$ [10]. Jamie Simpson [8] independently found a similar proof.

The Berger–Felzenbaum–Fraenkel revolution: from number theory to discrete geometry via the Chinese remainder theorem While it is true that the set of positive integers is an infinite set, a covering system is a finite object. In order to verify that a proposed covering system $\{a_i(m_i)\}_{i=1}^N$ is indeed one, it suffices to check that it covers all the integers n between 0 and $M-1$, where

$$M = \operatorname{lcm}(m_1, m_2, \ldots, m_N).$$

By the fundamental theorem of arithmetic

$$M = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

where $p_1, \ldots, p_k$ are primes and $r_1, \ldots, r_k$ are positive integers.

For the sake of simplicity, let's assume that M is square-free, i.e., all the exponents $r_1, \ldots, r_k$ equal 1. The same reasoning, only slightly more complicated, applies in the general case. Now we have $M = p_1 p_2 \cdots p_k$.

The ancient, but still useful, Chinese remainder theorem tells you that there is a bijection between the set of integers between 0 and $M-1$, which we shall denote $[0, M-1]$, and the Cartesian product of $[0, p_i - 1]$, $i = 1, \ldots, k$,

$$f : [0, M-1] \to \prod_{i=1}^{k} [0, p_i - 1],$$

defined by

$$f(x) := [x \pmod{p_1}, x \pmod{p_2}, \ldots, x \pmod{p_k}].$$

So each integer in $[0, M-1]$ is represented by a point in the $p_1 \times p_2 \times \cdots \times p_k$ k-dimensional discrete box $\prod_{i=1}^k [0, p_i - 1]$.

If $a(m)$ is a member of our covering system, then since m is a divisor of M, it can be written as a product of some of the primes in $\{p_1, \ldots, p_k\}$, say

$$m = p_{i_1} p_{i_2} \cdots p_{i_s}.$$

Let

$$m_{i_1} = a \pmod{p_{i_1}}, \quad m_{i_2} = a \pmod{p_{i_2}}, \quad \ldots, \quad m_{i_s} = a \pmod{p_{i_s}}.$$

It follows that the members of the congruence $a(m)$ correspond to the points in the $(k-s)$-dimensional *sub-box*

$$\{(x_1, \ldots, x_k) \in [0, p_1 - 1] \times \cdots \times [0, p_k - 1] \quad | \quad x_{i_1} = m_{i_1}, \ldots, x_{i_s} = m_{i_s}\}.$$

For example, if $M = 30 = 2 \cdot 3 \cdot 5$, the congruence class 7(10), corresponds to the one-dimensional sub-box (since $7 \pmod 2 = 1$ and $7 \pmod 5 = 2$)

$$\{(x_1, x_2, x_3) : x_1 = 1, 0 \le x_2 \le 2, x_3 = 2\}.$$

In other words, a covering system (with square-free M) is nothing but a way of expressing a certain k-dimensional discrete box as a union of sub-boxes. This was the beautiful insight of Marc Berger, Alex Felzenbaum, and Aviezri Fraenkel.

Erdős's famous problem and Bob Hough's refutation Erdős [6] famously asked whether there exists a distinct covering system

$$a_i \pmod{m}_i, \quad 1 \le i \le N, \quad m_1 < m_2 < \cdots < m_N,$$

with the smallest modulus, m_1, arbitrarily large.

As computers got bigger and faster, people (and their computers) came up with examples that progressively made m_1 larger and larger, and many humans thought that indeed m_1 can be made as large as one wishes. This was brilliantly refuted by Bob Hough [7] who proved that $m_1 \leq 10^{16}$. This is definitely not sharp, and the true largest m_1 is probably less than 1000.

Let's now move on from number theory to something apparently very different: logic!

Boolean functions

Let's recall some basic definitions. A *Boolean function* (named after George Boole [3]) of n variables is a function from $\{\text{false}, \text{true}\}^n$ to $\{\text{false}, \text{true}\}$. Altogether there are 2^{2^n} Boolean functions of n variables. Any Boolean function $f(x_1, \ldots, x_n)$, is determined by its *truth table*, or equivalently, by the set $f^{-1}(\text{true})$, one of the 2^{2^n} subsets of $\{\text{false}, \text{true}\}^n$.

The *simplest* Boolean functions are the *constant* functions **true** (the *tautology*) corresponding to the whole of $\{\text{false}, \text{true}\}^n$, and **false** (the *anti-tautology*) corresponding to the *empty set*.

In addition to the above constant Boolean functions, there are three *atomic* functions. The simplest is the *unary* function NOT, denoted by $\bar{x}$, that is defined by

$$\bar{x} = \begin{cases} \text{false}, & \text{if} \quad x = \text{true} \\ \text{true}, & \text{if} \quad x = \text{false}. \end{cases}$$

The two other fundamental Boolean functions are the (inclusive) OR, denoted by $\vee$, and AND, denoted by $\wedge$. The expression $x \vee y$ is true unless both x and y are false, and $x \wedge y$ is true only when both x and y are true.

By iterating these three operations on n variables, one can get many *Boolean expressions*, and each Boolean function has many possible expressions.

From now on we will denote, as usual, true by 1 and false by 0. Also let $x^1 = x$ and $x^0 = \bar{x} = 1 - x$.

One particularly simple type of expression is a (pure) *conjunction*. It is anything of the form (for some t, called its *size*),

$$x_{i_1}^{j_1} \wedge \cdots \wedge x_{i_t}^{j_t},$$

where $1 \leq i_1 < \cdots < i_t \leq n$ and $j_i \in \{0, 1\}$ for all $1 \leq i \leq t$.

Of interest to us is the type of expression called the *disjunctive normal form* (DNF). A DNF has the form

$$\bigvee_{i=1}^{N} C_i,$$

where each C_i is a pure conjunction.

Every Boolean expression corresponds to a unique function, but every function can be expressed in many ways, and even in many ways that are DNF. The most straightforward way is the *canonical DNF* form

$$\bigvee_{\{v \in f^{-1}(1)\}} \bigwedge_{i=1}^{n} x_i^{v_i}.$$

Note that a pure conjunction of length t

$$x_{i_1}^{j_1} \wedge \cdots \wedge x_{i_t}^{j_t}$$

corresponds to a *sub-cube* of dimension $n - t$, namely to

$$\{(x_1, \ldots, x_n) \mid x_{i_1} = j_1, \ldots, x_{i_t} = j_t\}.$$

Hence, one can view a DNF as a (usually not exact) *covering* of the set $f^{-1}(1)$ of truth-vectors by sub-cubes. In particular, a *DNF tautology* is a covering of the whole n-dimensional unit cube by lower-dimensional sub-cubes.

DNFs and the million dollar problem The most fundamental problem in theoretical computer science, the question of whether **P** is *not* **NP** (of course it is not, but proving it rigorously is another matter), is equivalent to the question of whether there exists a polynomial time algorithm that decides if a given disjunctive normal form expression is the *tautology* (i.e., the constant function 1). Of course, there is an obvious brute force algorithm: For each term, find the truth-vectors covered by it, take the union, and see whether it contains all the 2^n members of $\{0, 1\}^n$. But this takes *exponential* time and memory.

The covering system analog We can formulate a similar problem based on covering systems. Input a system of congruences

$$a_i \pmod{m_i} \quad 1 \le i \le N,$$

and decide, in *polynomial time*, whether it is a covering system. Initially it seems that we need to check infinitely many cases, but of course (as already noted above), it suffices to check whether every integer between 1 and $\operatorname{lcm}(m_1, \ldots, m_N)$ belongs to at least one of the congruences. This seems fast enough! Alas, the size of the input is the sum of the number of digits of the a_i's and m_i's. This is less than a constant times the *logarithm* of $\operatorname{lcm}(m_1, \ldots, m_N)$, so just like for Boolean functions, the naive algorithm requires time (and space) exponential in the *input size*.

Boolean function analogs of covering systems

We next consider Boolean function analogs of covering systems. The first one to consider such analogs was Melkamu Zeleke [11]. Here we continue his pioneering work. We saw that a DNF tautology is nothing but a covering of the n-dimensional unit cube $\{0, 1\}^n$ by sub-cubes. So it is the analog of a covering system.

The analog of *exact* covering systems is obvious: all the terms should cover disjoint sub-cubes. For example, when $n = 2$, (from now on xy means $x \wedge y$)

$$x_1x_2 \vee x_1\bar{x_2} \vee \bar{x_1}x_2 \vee \bar{x_1}\bar{x_2},$$

and

$$x_1 \vee \bar{x_1}x_2 \vee \bar{x_1}\bar{x_2},$$

are such.

In order to define *distinct* DNF, we define the *support* of a conjunction as the set of the variables that participate. For example, the support of the term $\bar{x_1}\bar{x_3}x_4x_6$ is the set $\{x_1, x_3, x_4, x_6\}$. In other words, we ignore the negations. For each t-subset of $\{x_1, \ldots, x_n\}$, there are 2^t conjunctions with that support. Geometrically speaking, two terms with the same support correspond to sub-cubes which are "parallel" to each other.

Note that the supports correspond to the modulus, m, and the assignments of negations (or no negation) corresponds to a residue class modulo m.

A DNF tautology is *distinct* if it has distinct supports.

An obvious example of a distinct DNF tautology in n variables is

$$\bigvee_{i=1}^{n} x_i \;\vee\; \wedge_{i=1}^{n} \bar{x}_i .$$

More generally, for every $1 \leq t \leq n$, $(t \neq n/2)$ the following is a distinct DNF tautology:

$$\left(\bigvee_{1 \leq i_1 < i_2 < \cdots < i_t \leq n} x_{i_1} \cdots x_{i_t} \right) \vee \left(\bigvee_{1 \leq j_1 < j_2 < \cdots < j_{n-t} \leq n} \bar{x}_{j_1} \cdots \bar{x}_{j_{n-t}} \right) .$$

This follows from the fact that by the pigeon-hole principle, every $0 - 1$ vector of length n has either at least t 1's or at least n-t 0's.

The Boolean analog of the Mirsky–Newman–Davenport–Rado theorem is almost trivial. First, suppose we have an exact DNF tautology where the largest support has size n. That corresponds to a point (a 0-dimensional sub-cube). If it is the only one, then since a conjunction of length t covers 2^{n-t} points, if all the other ones are strictly smaller than n, and since they are all disjoint, they cover an even number of points, hence there is no way that an exact DNF tautology would only have one term of size n.

If the largest size of a term is $<n$, then by projecting on appropriate sub-boxes one can reduce it to the former case, and see that it must have a mate.

The Boolean analog of the Erdős problem is true Taking n to be odd, the above DNF tautology with $t = (n-1)/2$ has "minimal moduli" (supports) of size $(n-1)/2$, and that can be made as large as one wishes.

First challenge This leads to a more challenging problem: For each specific n, how large can the minimum clause size, let's call it k, be in a distinct DNF tautology?

A simple *necessary condition*, on density grounds, is that

$$\sum_{i=k}^{n} \binom{n}{i} \frac{1}{2^i} \geq 1.$$

(Each subset of size i of $\{1, \ldots, n\}$ can only show up once and covers 2^{n-i} vertices of the n-dimensional unit cube. Now use Boole's inequality that says that the number of elements of a union of sets is less than or equal to the sum of their cardinalities.)

Let A_n be the largest such k. The first 14 values of A_n are

$$1, 1, 1, 2, 3, 4, 4, 5, 6, 7, 7, 8, 9, 10.$$

We were able to find such optimal distinct DNF tautologies for all $n \leq 14$ except for $n = 10$, where the best that we came up with was one that covers 1008 out of the 1024 vertices of the 10-dimensional unit cube, leaving 16 points uncovered, and for $n = 14$, where 276 out of the $2^{14} = 16{,}384$ points were left uncovered. See `out1.txt` in the supplementary materials.

Second challenge Another challenge is to come up with distinct DNF tautologies with all the terms of the *same* size. By density arguments, a necessary condition for the existence of such a distinct DNF tautology is

$$\binom{n}{m}\frac{1}{2^m} \geq 1.$$

Let B_m be the largest such m. The first 14 values are

$$0, 0, 1, 2, 3, 3, 4, 5, 6, 6, 7, 8, 9, 9.$$

For $n = 3$, where $B_3 = 1$, it is not possible, since $x_1 \vee x_2 \vee x_3$ can't cover everything. We were also unable to find such optimal DNF tautologies for $n = 5$, where $B_5 = 3$ and we had to leave one vertex uncovered, $n = 9$, (with $B_9 = 6$), where 13 vertices were left uncovered, and $n = 13$ (with $B_{13} = 9$) where $2^{13} - 8090 = 102$ vertices were left uncovered. For the other cases with $n \leq 14$, we met the challenge. See `out2.txt` in the supplementary materials.

Many more examples can be gotten from the Maple package `dt.txt` in the supplementary materials.

The general problem: covering a discrete box by non-parallel sub-boxes Let $\{a_i\}_{i=1}^{\infty}$ be a weakly increasing sequence of positive integers, with $a_1 \geq 2$.

Is it true that for every m there exists an n such that the box $[1, a_1] \times \cdots \times [1, a_n]$ can be covered by *non-parallel* sub-boxes, each of dimension $\leq n - m$?

We saw that for the Boolean case, with $a_i = 2$ for each i (and analogously, for each constant sequence), the answer is trivially *yes*.

On the other hand, if

$$\sum_{i=1}^{\infty} \frac{1}{a_i} < \infty,$$

the answer is *no*, since

$$\prod_{i=1}^{\infty} \left(1 + \frac{1}{a_i}\right) < \infty,$$

and by a density argument, all tails of the product will eventually be less than 1, so there is not enough room.

Regarding the original Erdős problem, Hough [7] proved the answer is *no* in the case with $a_i = p_i$, the sequence of prime numbers. (In fact, Hough proved the slightly harder result where the moduli are not necessarily square-free.) Here the sum of the reciprocals *almost* converges. The very naive Boole's inequality does not suffice to rule out a positive answer to the Erdős problem, but the Lovász local lemma suffices to do the job.

So in a way, the fact that $\{a_i\}$ was initially the sequence of primes was a red herring. In this general framework, what is important is the asymptotics of this sequence.

It would be interesting to see to what extent Hough's proof of impossibility extends to other sequences (a_i) for which the answer is neither an obvious *yes*, nor an obvious *no*.

REFERENCES

[1] Berger, M. A., Felzenbaum, A., Fraenkel, A. (1986). A nonanalytic proof of the Newman-Znam result for disjoint covering systems. *Combinatorica*. 6(3): 235–243. doi.org/10.1007/BF02579384

[2] Berger, M. A., Felzenbaum, A., Fraenkel, A. (1986). New results for covering systems of residue sets. *Bull. Amer. Math. Soc*. 14(1): 121–125. doi.org/10.1090/S0273-0979-1986-15414-5

[3] Boole, G. (1958). *An Investigation Into the Laws of Thought*. Mineola, NY: Dover. Reprint of the original 1854 edition.

[4] Delahaye, J.-P. (2017). Cinq énigmes pour la rentrée. *Pour Sci*. 479: 80–85.

[5] Erdős, P. (1950). On integers of the form $2^k + p$ and some related problems. *Summa Brasil. Math.* 2: 113–123.

[6] Erdős, P. (1952). On a problem concerning covering systems. *Mat. Lapok.* 4: 122–128.

[7] Hough, B. (2015). Solution of the minimum modulus problem for covering systems. *Ann. Math.* 181(1): 361–382. doi.org/10.4007/annals.2015.181.1.6

[8] Simpson, R. J. (1986). Exact covering of the integers by arithmetic progressions. *Discrete Math*. 59(1–2): 181–190. doi.org/10.1016/0012-365X(86)90079-8

[9] Winkler, P. (2007). *Mathematical Mind-Benders*. Wellesley, MA: A. K. Peters.

[10] Zeilberger, D. (2001). How Berger, Felzenbaum and Fraenkel revolutionized covering systems the same way that George Boole revolutionized logic. *Electron. J. Comb*. 8(2): A1.

[11] Zeleke, M. (1998). *Discrete Radon transform, covering congruences, and Boolean functions.* Ph.D. dissertation. Temple University, Philadelphia.

Summary. Bob Hough recently disproved a long-standing conjecture of Paul Erdős regarding covering systems. Inspired by his seminal paper, we describe analogs of covering systems to Boolean functions, and more generally, the problem of covering discrete hyper-boxes by non-parallel lower dimensional hyper-sub-boxes. We exhibit how the Erdős problem is a special case of this general setup, where the side lengths of the boxes are primes. We discover that the primes were red herrings. Indeed, given this general framework, we can prove the same results for sequences other than the prime numbers; we only need a weaker asymptotic condition.

ANTHONY ZALESKI (MR Author ID: 1013551) received his Ph.D. in mathematics from Rutgers University. His research involved the application of experimental math to problems in combinatorics. His advisor was none other than Doron Zeilberger. Anthony now works in finance.

DORON ZEILBERGER (MR Author ID: 186835) is a Board of Governors Professor at Rutgers University. His first mathematical love was Boolean functions, and when he was 18 years old, he rediscovered a way to simplify Boolean functions that turned out to be equivalent to the known Quine–McCluskey algorithm. It was fun returning to his first love in the writing of this paper.