Boolean Function Analogs of Covering Systems

Anthony ZALESKI and Doron ZEILBERGER

Abstract: 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-subboxes. We point out that very often primes are red herrings. This is definitely the case for covering system, and who knows, perhaps also for the Riemann Hypothesis.

Prime Numbers are Sometimes Red Herrings

The great French mathematical columnist Jean-Paul Delahaye [D] recently posed the following brain-teaser, adapting a beautiful puzzle, of unknown origin, popularized by Peter Winkler in his wonderful book [W] (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, where 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 lovely 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 they 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).

This variation, due to Delahaye, is **much** harder than the original version posed in [W], 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. Something analogous happened to the great Paul Erdős, the patron saint of combinatorics and number theory, who introduced **covering systems**.

Covering Systems

In 1950, Paul Erdős [E1], introduced the notion of **covering systems**. A *covering system* is a finite set of arithmetical progressions

$$\{ a_i \,(\, mod\, m_i) \quad | \quad 1 \leq i \leq N \} \quad ,$$

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

$$\{0\,(\, mod\, 1)\} \quad ,$$

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

$$\{ 0\,(\, mod\, 2) \quad , \quad 1\,(\, mod\, 2)\} \quad ,$$

and

$$\{ 0\,(mod\, 5) \quad , \quad 1\,(mod\, 5) \quad , \quad 2\,(mod\, 5) \quad , \quad 3\,(mod\, 5) \quad , \quad 4\,(mod\, 5)\,\} \quad ,$$

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

$$\{ 0\,(mod\, 2) \quad , \quad 1\,(mod\, 4) \quad , \quad 3\,(mod\, 4)\,\} \quad .$$

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 $a\,(\,mod\, b)$.]

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

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

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 in [E2]) 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 $m_1 \leq m_2 \leq \ldots \leq m_N$, 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 [Zei1] 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, Fraenkel ([BFF1][BFF2]), and exposited in [Zei1]. In fact, they proved the more general Znam theorem that asserts that the highest moduli shows up at least p times, where p is the smallest prime dividing $lcm\,(\,m_1, \ldots, m_N\,)$. Jamie Simpson ([S]) independently found a similar proof, but unfortunately chose not to express it in the evocative geometrical language.

The Berger-Felzenbaum revolution: From Number Theory to Discrete Geometry via the Chinese Remainder Theorem

While it is a sad truth that the set of positive integers is an *infinite* set, a covering system is a **finite** object. In order to verify that a 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

$$M \;=\; lcm\,(\,m_1, m_2, \ldots, m_N\,) \quad .$$

By the fundamental theorem of arithmetic

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

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

$$M = p_1 p_2 \cdots p_k \quad .$$

The ancient, but still useful, **Chinese Remainder Theorem** tells you that there is a bijection between the set of integers between 0 and $M-1$, let's call it $[0, M-1]$, and the Cartesian product of $[0, p_i - 1]$, $i = 1 \ldots k$.

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

defined by

$$f(x) := \;[x \; mod \; p_1 \, , \, x \; mod \; p_2 \, , \quad \ldots \quad , x \; mod \; p_k \,] \quad .$$

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

If $a\,(\,m\,)$ is a member of our covering system, 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

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

Let

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

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

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

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

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

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, nicely exposited in [Zeil1].

Erdős's Famous Problem and Bob Hough's Refutation

Erdős ([E2]) famously asked whether there exists a distinct covering system

$$a_i(\, mod \, m_i) \quad , \quad 1 \le i \le N \quad , \quad m_1 < m_2 < \ldots < m_N \quad ,$$

with the smallest modulo, 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 thoughts that indeed m_1 can be made as large as one wishes. This was brilliantly refuted by Bob Hough ([H]) who proved that $m_1 \le 10^{16}$. 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 ([Bo])) of n variables is a function from $\{False, True\}^n$ to $\{False, True\}$. 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 $f^{-1}(True)$, one of the 2^{2^n} subsets of $\{False, True\}^n$.

The *simplest* Boolean functions are the **constant** Boolean functions **True** (the *tautology*) corresponding to the whole of $\{False, True\}^n$, 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

$$\bar{x} \; = \begin{cases} False \, , & if \quad x = True; \\ True \, , & if \quad x = False \, . \end{cases}$$

The two other fundamental Boolean functions are the (inclusive) **OR**, denoted by $\vee$ and **AND**, denoted by $\wedge$. $x \vee y$ 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 **conjunction** (also called *term*). It is anything of the form, for some t, called its **size**,

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

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

Of interest to us in this article is the type of expression called the *Disjunctive Normal Form* (DNF) (featured prominently, along with its *dual*, *Conjunctive Normal Form*, (CNF), in Norbert Blum's brave attempt ([Bl], see also [Zeil2])). It simply has the form

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

where each C_i are pure conjunctions.

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. One way that is the most straightforward way is the **canonical DNF** form

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

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

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

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.

Digression: 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 *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 **exponential memory**.

The Covering System Analog

Input a system of congruences

$$a_i \,(\,mod\, m_i\,) \quad , \quad 1 \le i \le N \quad ,$$

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 $lcm\,(\,m_1, \dots, m_N)$ 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 and this is less than a constant times the *logarithm* of $lcm\,(\,m_1, \dots, m_N)$, so just like for Boolean functions, the naive algorithm is exponential time (and space) in the *input size*.

We next consider Boolean function analogs of covering systems. The first one to consider such analogs was Melkamu Zeleke ([Zel]). Here we continue his pioneering work.

Boolean Function Analogs of Covering Systems

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 $x \wedge y$)

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

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

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 $\{x_1, \dots, x_n\}$ 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 modulo, 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

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

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

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

This follows from the fact that by the pigeon-hole principle, every $0-1$ vector of length n either has $\ge t$ 1's or $\ge n-t$ 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 subcube). 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 obviously 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, in a distinct DNF tautology, be?

An obvious **necessary condition**, on **density grounds**, is that

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

(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 $\le$ than the sum of their cardinalities).

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

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

We were able to find such optimal distinct DNF tautologies for all $n \le 14$ 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 $2^{14} = 16384$ points were left uncovered.

See the output file

`http://sites.math.rutgers.edu/~zeilberg/tokhniot/odt2.txt` .

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

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

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

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

Obviously 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 the output file

`http://sites.math.rutgers.edu/~zeilberg/tokhniot/odt1.txt` .

Supporting Maple Packages and Output

Many more examples can be gotten from the Maple package

- `http://www.math.rutgers.edu/~zeilberg/tokhniot/dt.txt` ,

whose output files are available from the *front* of this article

`http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/dt.html` .

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 $[1, a_1] \times \ldots [1, a_n]$ 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 obviously **yes**.

On the other hand, if

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

the answer is obviously **no**, since

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

and by a trivial 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 ([H]) 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 [that is also fairly weak; for example, it barely improves the lower bounds for the Ramsey numbers] suffices to do the job.

So prime numbers were indeed **red herrings**. All that was needed was their asymptotic behavior. 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. We also desperately need more powerful sieves than Lovász, Brun, Selberg, and the other known sieves, which, with lots of ingenuity, got close to the twin-prime conjecture (Yitang Zhang); but even the still open twin-prime conjecture, and the Goldbach conjecture, are much weaker than the true state of affairs.

Even though the Bonferroni sieve is fairly weak, it can often decide *satisfiability* (both positively and negatively). See the article [Za] by the first-named author.

References

[BFF1] Marc A. Berger, Alexander Felzenbaum and Aviezri Fraenkel, *A nonanalytic proof of the Newman-Znam result for disjoint covering systems*, Combinatorica **6** (1986), 235-243.

[BFF2] Marc A. Berger, Alexander Felzenbaum and Aviezri Fraenkel, *New results for covering systems of residue sets*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), 121–126.

[Bl] Norbert Blum, *A solution of the P versus NP problem*,
`https://arxiv.org/abs/1708.03486` .

[Bo] George Boole, L.L.D., "*Investigations of THE LAWS OF THOUGHT, Of Which Are Founded The Mathematical Theories of Logic and Probabilities*", Macmillan, 1854. Reprinted by Dover, 1958.

[D] Jean-Paul Delahaye, *Cinq énigmes pour la rentrée*, Logique et Calcul column, *Pour La Science*, No. **479** (Sept. 2017), 80-85.

[E1] Paul Erdős, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113-123.

[E2] Paul Erdős, *On a problem concerning covering systems* (Hungarian, English summary), Mat.

Lapok **3** (1952), 122-128.

[H] Bob Hough, *Solution of the minimum modulus problem for covering systems*, Ann. Math. **181** (2015), 361-382. `https://arxiv.org/abs/1307.0874` .

[S] Jamie Simpson, *Exact covering of the integers by arithmetic progressions*, Discrete Math. **59** (1986), 181-190.

[SZel] Jamie Simpson and Melkamu Zeleke, *On disjoint covering systems with exactly one repeated modulus*, Adv. Appl. Math. **23** (1999), 322-332.

[W] Peter Winkler, "*Mathematical Mind-Benders*," A.K. Peters/CRC Press, 2007.

[Za] Anthony Zaleski, *Solving satisfiability using inclusion-exclusion*,
`http://sites.math.rutgers.edu/~az202/Z/sat/sat.pdf` . Maple package:
`http://sites.math.rutgers.edu/~az202/Z/sat/sat.txt` .

[Zei1] Doron Zeilberger, *How Berger, Felzenbaum and Fraenkel revolutionized Covering Systems the same way that George Boole revolutionized Logic*, Elect. J. Combinatorics **8(2)** (2001) (special issue in honor of Aviezri Fraenkel), A1.
`http://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/af.html` .

[Zei2] Doron Zeilberger, *CNF-DNF and all that (Videotaped Lecture)*, available from
`http://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/CNFDNFLecture.html` .

[Zel] Melkamu Zeleke, *Ph.D. dissertation*, Temple University, 1998.

Anthony Zaleski, Department of Mathematics, Rutgers University (New Brunswick), Hill Center-Busch Campus, 110 Frelinghuysen Rd., Piscataway, NJ 08854-8019, USA.
Email: `az202 at math dot rutgers dot edu` .

Doron Zeilberger, Department of Mathematics, Rutgers University (New Brunswick), Hill Center-Busch Campus, 110 Frelinghuysen Rd., Piscataway, NJ 08854-8019, USA.
Email: `DoronZeil at gmail dot com` .

Jan. 15, 2018