How Berger, Felzenbaum and Fraenkel Revolutionized COVERING SYSTEMS The Same Way that George Boole Revolutionized LOGIC

Doron ZEILBERGER [1]

leMori veRabi Aviezri Fraenkel, who taught me that Games are Math and Math is a Game

Abstract: The Berger-Felzenbaum-Fraenkel approach to Covering Systems is exposited. In particular their gorgeous proof of the famous $a_n = a_{n-1}$ theorem for exact covering systems (found independently by Jamie Simpson), is reviewed, and the analogy of their approach to Boolean tautologies in Disjunctive Normal Form is pointed out.

Preface

There is more than one way to contribute to the preservation of the human species. The *explicit* way is to marry and have children, and if your children turn out to be good, you can and should feel proud. But, a more efficient way is to be a *matchmaker*, and make good matches, and if the couples that you have introduced to each other turn out to have brilliant children, then you may brag about them as though they were your own.

This also applies to math. If you have introduced (directly or indirectly) Dr. Reuven to Professor Simeon, and cast the deciding vote in the committee that admitted Mr. Levi to the Ph.D. program, then you are justified in feeling enormous satisfaction when the Reuven-Simeon-Levi collaboration leads to a major breakthrough in a whole area of mathematics. If this collaboration also lead to a MOST BEAUTIFUL proof, from the BOOK of BOOKS, sought out for many years by the BOOK's proposer, and begged by him in hundreds of lectures, then you can REALLY gloat.

This happened to me with
Reuven=Marc Berger, *Simeon=Aviezri Fraenkel,* *Levi=Alex Felzenbaum* .

The area that they revolutionized is *covering systems*, and the beautiful proof that they found is the long-sought-for elementary proof of the Davenport-Rado-Mirsky-Newman $a_n = a_{n-1}$ theorem.

I will tell this story, and the math, later in this article. But let's start at the beginning.

[1] Department of Mathematics, Temple University, Philadelphia, PA 19122, USA. `zeilberg@math.temple.edu` `http://www.math.temple.edu/~zeilberg/` . April 7, 2000. Supported in part by the NSF.

1650 Years Ago

In *Sun Tsu Suan Ching* (Master Sun's Arithmetic Manual) there is the following problem:

There is an unknown number of objects. When counted in "threes", the remainder is 2*; when counted in "fives", the remainder is* 3*; and when counted in "sevens", the remainder is* 2*. How many objects are there?"*

This means that we have to solve the congruences $x \equiv 2 (mod\, 3)$, $x \equiv 3 (mod\, 5)$, $x \equiv 2 (mod\, 7)$, and the answer is $x \equiv 23 (mod\, 105)$.

A much larger example appeared 900 years later.

750 Years Ago

The Ta Yen Algorithm by Chin Chiu Shao:

Three thieves A,B,C, each steal three (identical) full rice vessels.

Thief A used a 'horse ladle' (19 Ko), and got 1 Ko left-over.

Thief B used his 'wooden shoe' (17 Ko), and got 14 Ko left-over.

Thief C used a 'bowl' (12 Ko), and got 1 Ko left-over.

How many Kos in a rice vessel?

Here we have to solve $x \equiv 1(\, mod\, 19 \,)$, $x \equiv 14(\, mod\, 17)$, $x \equiv 1(\, mod\, 12 \,)$, and the smallest answer turns out to be $x = 3193$.

The *Chinese Remainder Theorem* tells us that we can always solve any system of congruences

$$x \equiv b_i(\, mod\, a_i) \quad , \quad i = 1 \dots k \quad ,$$

whenever $a_1, \dots, a_k$ are pairwise relatively prime, and the answer is unique modulo $lcm(a_1, \dots, a_k)$.

In particular if $N = p_1 \dots p_k$ is square-free, then the map

$$x \; \rightarrow \; (x \, mod \, p_1, x \, mod \, p_2, \dots, x \, mod \, p_k)$$

is one-to-one between $[0, N-1]$ and $[0, p_1 - 1] \times [0, p_2 - 1] \times \dots \times [0, p_k - 1]$.

Almost 150 Years Ago

George Boole published *The Laws of Thought* where he did to Propositional Logic what Descartes did to Geometry: he turned it into Algebra, which today is justifiably called *Boolean Algebra*. This, in turn, via the notion of *truth table*, ultimately became *Geometry*, albeit of the discrete kind.

Here are some "sound bites" from his magnificent opus [B].

" That Language is an instrument of Human reason, and not merely a medium for the expression of thought, is a truth generally admitted."

" How is it possible to make an assertive proposition out of a series of denials or negations? ... For example: 'There are no men who are not fallible= All Men are fallible'. "

" ... In Logic ... Truth is made manifest in all its generality, by reflecting upon a single instance of its application."

In fact, one has to reflect on all 2^n possible true-false assignments, and if a proposition $f(x_1, \dots, x_n)$, that only uses 'or', 'and' and 'not' is always true upon all 2^n possible assignments of true-false values into the atomic statements $x_1, \dots, x_n$, then it is a *tautology*. Otherwise you can *identify* the *Boolean function* with its set of truth-vectors, $S = \{(a_1, \dots, a_n)\}$, and write f in *complete Disjunctive Normal Form*

$$f(x_1, \dots, x_n) = \bigvee_{(a_1,\dots,a_n)\in S} x_1^{a_1} \dots x_n^{a_n} \quad ,$$

1 stands for 'true', 0 for 'false', $x^1 = x$, and $x^0 = \overline{x}$.

There are *lots* of Boolean functions, in fact 2^{2^n} of them. Shannon used their abundance to show that most Boolean functions are 'complicated', i.e., need super-polynomially many gates to be realized, since the number of functions computed by polynomially-bounded many gates is just exponential, not doubly so.

In particular, there is only one way to write the Boolean function 1 (THE tautology), in complete Disjunctive Normal Form:

$$1 = \bigvee_{a_1\in\{0,1\}} \dots \bigvee_{a_n\in\{0,1\}} x_1^{a_1} \dots x_n^{a_n} \quad .$$

But, if you do not insist on *completeness*, only on it being in *disjunctive normal form*, then there are many ways to write 1, including 1 itself. For example, if $n = 3$ then the following are tautologies in Disjunctive Normal Form (DNF).

$$x_1 \vee x_2 \vee x_3 \vee \overline{x}_1\overline{x}_2\overline{x}_3 \quad , \tag{aleph}$$

$$x_1\overline{x}_2 \vee x_2\overline{x}_3 \vee x_3\overline{x}_1 \vee \overline{x}_1\overline{x}_2\overline{x}_3 \vee x_1x_2x_3 \quad , \tag{bet}$$

$$x_1\overline{x}_2 \vee x_1x_2 \vee \overline{x}_1 \vee x_1x_3 \quad . \tag{gimel}$$

So, thanks to Boole, a DNF-tautology is a way of writing the discrete n-dimensional unit cube as a union of lower-dimensional sub-cubes. The term $x_{i_1}^{a_1} \dots x_{i_r}^{a_r}$ represents the $(n-r)$-dimensional unit cube consisting of those points for which $x_{i_1} = a_1, \dots, x_{i_r} = a_r$.

Let's call the *support* of an elementary conjunction $x_{i_1}^{a_1} \dots x_{i_r}^{a_r}$ (equivalently an $(n-r)$-dimensional subcube: $x_{i_1} = a_1, \dots, x_{i_r} = a_r$), the set $\{i_1, \dots, i_r\} \subset \{1, \dots, n\}$.

A DNF-tautology is *exact* if all the terms are disjoint, i.e. the covering of the unit cube is in fact a *partition.* For example the DNF-tautology (*bet*) is exact. It is *distinct* if all the supports are distinct, in other words none of the subcubes are 'parallel'. For example (*aleph*) is a distinct DNF-tautology. But (*gimel*) is neither exact nor distinct.

Utterly Trivial Observation: If an exact DNF-tautology contains at least one term that is a point (0-dimensional subcube), then it must contain at least two.

Proof: The cardinality of an r-dimensional cube is 2^r. If $r > 0$, then it is even. Since the cardinality of the unit n-dimensional cube is 2^n, and hence even, and since even minus even is even, it follows that the number of singletons is even. Since it is at least 1, by assumption, it must be at least 2. $\square$

What if the exact DNF-tautology does not have any singletons? Then it contains terms of maximal support, say a term $\prod_{i \in S} x_i^{a_i}$, where there are no terms whose support T strictly contains S. Then if follows immediately from the above utterly trivial observation that there must be at least another term whose support is S. This follows by considering the induced DNF-tautology on the variables in S, obtained by intersecting with $x_j = 0$, $j \in \{1, \dots, n\} \backslash S$ (i.e. "projecting" on that $|S|$-dimensional subcube). This turns the term $\prod_{i \in S} x_i^{a_i}$ into a point, and it follows from the above utterly trivial observation that it has at least one friend. Now that friend must be the 'shadow' (i.e. projection) of another term whose support is S, in the original DNF-tautology, or else S would not be maximal.

It follows in particular that you *can't have the cake and eat it too*, i.e. an exact DNF-tautology can't also be distinct.

To summarize: George Boole reduced propositional logic to algebra, and hence (via the notion of truth table introduced by Wittgenstein), to discrete geometry. A DNF-tautology is nothing but a covering of the n-dimensional unit cube $\{0,1\}^n$ by lower-dimensional cubes.

About 50 Years Ago

Erdős Pál [E] introduced the notion of *covering system*, a finite set of infinite arithmetical progressions

$$x \equiv b_i \,(mod\, a_i) \quad , \quad i = 1, \ldots, n \quad ,$$

whose union consists of all natural numbers.

For example: $\{x \equiv 0\,(\,mod\,2), x \equiv 1\,(\,mod\,2)\}$, $\{x \equiv 0\,(\,mod\,2\,), x \equiv 1\,(\,mod\,4), x \equiv 3\,(\,mod\,4)\}$, and

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

A covering system is called *exact* (ECS) if none of the arithmetical progressions overlap, i.e. for $1 \leq i < j \leq n$, $b_i\,(mod\,a_i)$ and $b_j\,(mod\,a_j)$ are always disjoint. A covering system is called *distinct* (DCS) if all the moduli a_i are different. The first two examples above are exact (but of course not distinct), while the third example is distinct (but not exact).

In his 1952 article [E], Erdős described a beautiful proof found by Mirsky and (Donald) Newman, and independently, by Davenport and Rado, that the two top-moduli of an ECS must be identical, i.e. if $b_1(mod\ a_1), \ldots, b_n(mod\ a_n)$ partition the integers, and $a_1 \leq a_2 \leq \ldots \leq a_n$, then we must have $a_{n-1} = a_n$. Their proof is a true gem. It goes as follows. The ECS-condition translates to the identity

$$\frac{1}{1-z} = \sum_{i=1}^{n} \frac{z^{b_i}}{1-z^{a_i}} \quad . \qquad (MNDR)$$

Indeed every monomial appears exactly once both on the left and the right when we Taylor-expand about $z=0$. Let ω be an a_n-th primitive root of unity. Now let $z \to \omega$. If $a_{n-1} < a_n$, then the left side and the first $n-1$ terms of the right side converge to a finite number, while the last term on the right blows up. Contradiction. Now this proof is definitely in the BOOK, but not in MY BOOK! As beautiful as it is, it is *analytical*, and uses fictional notions like complex numbers and limits, while the statement is purely elementary. Just like the Prime Number Theorem.

Erdős realized this and in many talks raised the question of finding an *elementary* proof of this theorem.

20 Years Ago: Marc Berger

In 1980, after four years as a postdoc in the States, I came back to the Weizmann Institute, where I got my Ph.D. in 1976, with the intention to stay. One of my positions was at Georgia Tech (1978-1979), where I met and befriended a remarkable and (then) young faculty member, Marc Berger. Marc was indeed a prodigy, and the chair at the time, the late Les Karlovitz, was often raving about him. Marc is not only a mathematical genius, but also a very talented pianist and erudite *talmid khacham*. He was also very versatile in his mathematical interests, and did both *pure* 'Radical Calculus', that he invented in collaboration with Alan Sloan, and very *applied* math, consulting for industry. He was also "*Black-Scholes* when *Black-Scholes* wasn't yet cool", and gave a fascinating series of talks about using the Ito calculus to price options, way back in 1978.

In 1980, Marc visited Israel, and looked me up. He told me that in his dissertation he used and generalized early work of my advisor, Harry Dym. So I introduced them to each other, and Harry was so impressed that he practically hired him on the spot, first as a visitor, and later on tenure-track.

Once Marc moved to Rehovot, he went to *shul* (of course), and who did he meet there , and very soon became good friends with? Aviezri Fraenkel! Now both Marc and Aviezri are very friendly and social people, who enjoy collaboration. So Aviezri told him about covering systems and about the many open problems in the field, and before you could say *shma Israel*, they started to collaborate. Soon they were joined by a 'junior partner'.

18 Years Ago: Alexander Felzenbaum

A young *ole khadash* (emigré) from Russia, Alexander Felzenbaum applied for admission to the graduate program at the Weizmann Institute. He seemed very bright and creative *but* (in fact I should say *hence*) non-standard, with a somewhat mixed record. So it was decided that he should have an oral entrance examination/interview in front of an admission committee. The committee consisted of Aviezri Fraenkel, Amir Pnueli (of temporal logic fame, 1996 Turing Award winner), and myself. The outcome of the interview was also mixed. Aviezri had some doubts, Amir abstained, but I was very favorable, and succeeded in convincing Aviezri and Amir about the potential of Alexander.

So, I believe that I deserve some credit in my implicit part in hiring Marc and my explicit part in admitting Alexander. To my great satisfaction this led to a revolution in covering systems, that was based on a very ancient idea, mentioned at the beginning, that of the Chinese Remainder Theorem (CRT).

14 ± 2 Years Ago

Consider a covering system $b_i(mod\, a_i), i = 1, \ldots, n$. Let $N = lcm(a_1, \ldots, a_n)$, and assume for now that N is square-free, and hence can be written as

$$N = \prod_{i=1}^{k} p_i \quad .$$

Recall that by the CRT, there is a one-one correspondence between the set of integer mod N and the set of points of the k-dimensional discrete box $[0, p_1 - 1] \times \ldots \times [0, p_k - 1]$, given by

$$b \rightarrow (b \; mod \; p_1, b \; mod \; p_2, \ldots, b \; mod \; p_k) \quad . \qquad (CRT)$$

For example, if $N = 30$ then 10 goes to the point $(0, 1, 0)$, 17 goes to the point $(1, 2, 2)$, and 29 goes to the point $(1, 2, 4)$.

What does a congruence $b \; (mod \; m)$, $m|N$ correspond to? If $m = p_{i_1} \ldots p_{i_r}$, then by (CRT) applied to m, the set of integers mod N that obey $x \equiv b(mod \; m)$, correspond to the points in the discrete box $[0, p_1 - 1] \times \ldots \times [0, p_k - 1]$ for which

$$x_{i_1} = b \; mod \; p_{i_1}, \quad x_{i_2} = b \; mod \; p_{i_2} \quad , \ldots , \quad x_{i_r} = b \; mod \; p_{i_r} \quad .$$

For example, if $N = 30$, then the congruence $1(mod\, 2)$ corresponds to $\{x_1 = 1\}$, the congruence $3(mod\, 5)$ corresponds to $\{x_3 = 3\}$, while $7(mod\, 10)$ corresponds to $\{x_1 = 1, x_3 = 2\}$, and $5(mod\, 6)$ corresponds to $\{x_1 = 1, x_2 = 2\}$, etc.

So just like in Boolean algebra, a DNF-tautology is *nothing but* a covering of the n-dimensional unit cube $[0, 1]^n$ by subcubes, Berger, Felzenbaum and Fraenkel realized that a covering system (for square-free N, see later about the general case) is *nothing but* a covering of the box $[0, p_1 - 1] \times \ldots \times [0, p_k - 1]$ by lower-dimensional sub-boxes! If the covering system is exact then we have a partition, if it is distinct, then we can't have 'parallel sub-boxes'.

Let $b_i(mod \; a_i), i = 1 \ldots n$, with $a_1 \leq \ldots \leq a_n$, be an ECS, and let $N = lcm(a_1, \ldots, a_n)$. Assume that $a_n = N$, i.e. one of the sub-boxes participating in the covering is 0-dimensional (a point). Can it be the only one? Of course not!, and for the same trivial reason as in the Boolean case. But first we have to go to Sodom and trim our box $[0, p_1 - 1] \times \ldots \times [0, p_k - 1]$ into a cube 'isomorphic' to $[0, p_1 - 1]^k$, making sure that it includes the above-mentioned point (there are many ways of doing it!). Now the original partition of the box into sub-boxes induces, by intersection, a partition of the cube $[0, p_1 - 1]^k$ into sub-cubes. Since all r-dimensional sub-cubes ($r > 0$) contain p_1^r points, whose number is divisible by p_1, and ditto for the number of points in $[0, p_1 - 1]^k$, it follows that the number of 0-dimensional subcubes is also divisible by p_1, and since it is at least 1, by assumption, it must be at least p_1. Since these are all points, they must already exist in the original partition of $[0, p_1 - 1] \times \ldots \times [0, p_k - 1]$. So Berger, Felzenbaum, and Fraenkel gave us more than we bargained for! Not just one extra point (congruence mod N), but $p_1 - 1$ more.

Now this stronger result was already known, due independently to (Morris) Newman and Znam, but their proof was *analytical*, and *much more complicated* than the Mirsky-(Donald) Newman-Davenport-Rado proof.

What if N is not square-free?

The most extreme case is a pure prime power, $N = p^r$. Here we need something even simpler than the Chinese Remainder Theorem, namely base-p-representation. Every integer b, between 0 and $p^r - 1$ can be written in base p:

$$b = \sum_{j=0}^{r-1} b_j p^j \quad ,$$

with $0 \leq b_j < p$. Hence b is mapped to the point $(b_{r-1}, \ldots, b_0)$ of the r-dimensional cube $[0, p-1]^r$. Now a congruence b_0 mod p corresponds to those points whose last coordinate ("digit") is b_0. A congruence $b_1 p + b_0$ mod p^2 corresponds to those points for which $x_{r-1} = b_1$ and $x_r = b_0$ etc. So in this case every congruence corresponds to a sub-box, but not usually vice-versa. Only sub-boxes of the form $x_m = b_{r-m}, x_{m+1} = b_{r-m-1}, \ldots, x_r = b_0$, i.e., whose support has the form $\{m, m+1, \ldots, r\}$, are admissible.

In the general case, when

$$N = \prod_{i=1}^{k} p_i^{m_i} \quad ,$$

BFF combine the two methods, mapping $[0, N-1]$ onto the box

$$[0, p_1 - 1]^{m_1} \times \ldots \times [0, p_k - 1]^{m_k} \quad ,$$

by first mapping x to $(x \, mod \, p_1^{m_1}, \ldots, x \, mod \, p_k^{m_k})$, and then further splitting the i^{th} coordinate into m_i coordinates, according to base p_i, $i = 1, \ldots, k$, as described above. Once again an exact covering system corresponds to a partition of the above box into sub-boxes but not all sub-boxes are allowed, but that does not change the beautiful BFF argument above.

What if $a_n < N$?, i.e. all the sub-boxes in the induced partition have non-zero dimension. Then we can project on an appropriate sub-box, just as we did in the Boolean case, and then use the above argument. So this concludes the gorgeous proof of [BFF1]. $\square$

Jamie Simpson's Independent Discovery of this Stunning Proof

At about the same time, Jamie Simpson also found essentially the same proof, but his proof was a little awkward, since he did not use any geometrical notions; everything was in terms of 'numbers'. I asked him about it, and he replied that he always had the geometrical picture in his mind, but felt that it was more 'elementary' not to use the language of geometry, so he translated everything back to integers, making the presentation less transparent.

This reminds me that some people speculate that the Ancient Greeks, at least by Pappus's time, knew analytical geometry, but did not consider it legitimate, so they translated back-and-forth into synthetic proofs, not telling anyone that they 'cheated'.

The Berger-Felzenbaum-Fraenkel Revolution

Marc, Alex, and Aviezri did much more with their approach. They found lots of new results and solved several open problems. See [BFF2] and its many references.

−50 Years Ago

I believe that the BFF *paradigm shift* is going to be even more significant in the future. Pointing out analogies between different areas of math leads to revolutions. Let me just cite Rota's "observation" that the concept of Möbius inversion, originally introduced in 1832 in number theory, when properly generalized, is a pillar in the Foundations of Combinatorial Theory.

Any question in covering systems has its Boolean analog and vice-versa. This leads to interesting new questions in both areas. In particular, Satisfiability, and finding minimal DNFs for Boolean functions, have their covering systems analogs. My former student, Melkamu Zeleke, made a start in these investigations ([Z]), and in a brilliant paper with Jamie Simpson ([SZ]) a previous record of BFF was broken. I am sure that the future will bring many more applications and insights that stem from the marvelous Berger-Felzenbaum-Fraenkel approach.

Acknowledgement: I wish to thank the two referees for numerous suggestions and corrections.

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.

[B] 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.

[E] Paul Erdős, *On a problem concerning covering systems*, (Hungarian, English summary), Mat. Lapok. **3** (1952), 122-128.

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

[SZ] Jamie Simpson and Melkamu Zeleke, *On disjoint covering systems with exactly one repeated modulus*, Advances in Applied Mathematics **23** (1999), 322-332.

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