THE BULLETIN OF SYMBOLIC LOGIC
Volume 15, Number 3, Sept. 2009

ENUMERATING TYPES OF BOOLEAN FUNCTIONS

ALASDAIR URQUHART

Abstract. The problem of enumerating the types of Boolean functions under the group of variable permutations and complementations was first stated by Jevons in the 1870s, but not solved in a satisfactory way until the work of Pólya in 1940. This paper explains the details of Pólya's solution, and also the history of the problem from the 1870s to the 1970s.

§1. Introduction. The problem of counting the number of possible propositions in a given set of variables is one of the oldest in combinatorics. In his polemical essay directed against the Stoics, entitled "On Stoic Self-Contradictions" (*De Stoicorum Repugnantiis*, 29. 1047 C-E) Plutarch makes the following intriguing remarks about the Stoic philosopher and logician Chrysippus (circa 282–206 B.C.):

> He says himself that the number of conjunctions produced by means of ten propositions exceeds a million, though he had neither investigated the matter carefully by himself nor sought out the truth with the help of experts. ... Chrysippus is refuted by all the arithmeticians, among them Hipparchus himself who proves that his error in calculation is enormous if in fact affirmation gives 103,049 conjoined propositions and negation 310,952 [38, p. 527].

In his history of Greek mathematics, Sir Thomas Heath remarks that "it seems impossible to make anything of these figures" [22, Vol. II, p. 256], while William and Martha Kneale remark: "It is difficult to make any satisfactory sense of the passage" [28, p. 162]. In 1958 Biermann and Mau made an attempt [4] at a solution, though their explication did not succeed in reproducing either of Hipparchus's numbers. In the first volume of his well known text on combinatorics [51, p. 51], Richard P. Stanley posed the problem of making sense of Plutarch's statement.

Finally, in January 1994, David Hough (who was a graduate student in mathematics at George Washington University at the time), inspired by Stanley's statement of the problem, found what is undoubtedly the correct

Received January 24, 2009.

1079-8986/09/1503-0001/$3.70

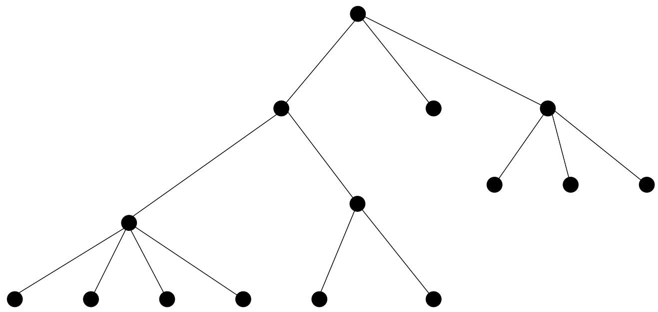

FIGURE 1. A planar tree with ten leaves.

solution to the puzzle, at least as far as the first of Plutarch's mysterious numbers is concerned. He noticed that this is exactly the tenth Schröder number! To explain the significance of his discovery, we need first to outline a little of the Stoic theory of propositions.

The Stoic logicians divided propositions into atomic ("This man is walking", "Socrates is sitting") and molecular. Molecular propositions are formed from atomic propositions using connectives such as disjunction, conjunction and negation [32]. Although contemporary logicians typically think of conjunction as a binary connective, the Stoics considered it as a connective of indefinite arity, so that it could conjoin two, three, or more propositions, as O'Toole and Jennings emphasize in their survey of Stoic logic [36, pp. 500–503].

Given this conception of proposition, it is not hard to see what might be meant by a conjunction produced by a given number of atomic propositions. For example, with four atomic propositions p, q, r, s, there are exactly 11 possible conjunctions: $(p \wedge q \wedge r \wedge s)$, $((p \wedge q) \wedge r \wedge s)$, $(p \wedge (q \wedge r) \wedge s)$, $(p \wedge q \wedge (r \wedge s))$, $((p \wedge q \wedge r) \wedge s)$, $(p \wedge (q \wedge r \wedge s))$, $(((p \wedge q) \wedge r) \wedge s)$, $((p \wedge (q \wedge r)) \wedge s)$, $((p \wedge q) \wedge (r \wedge s))$, $(p \wedge ((q \wedge r) \wedge s))$, and $(p \wedge (q \wedge (r \wedge s)))$. In other words, there are 11 possible bracketings of a sequence of four propositions, where the parentheses can enclose two or more members of the sequence. The number of possible bracketings of a sequence of length n is the nth Schröder number, $s(n)$—alternatively, it is the number of possible planar trees with n leaves, where each interior node has two or more descendants. For many more references on these numbers, the reader can consult the *Encyclopedia of Integer Sequences* [50], where the sequence is M2898; the on-line *Encyclopedia*, where the sequence is A001003, provides dozens of references and links to information about this famous sequence.

Hough's discovery that the first number of Plutarch is the tenth Schröder number, $s(10)$, fits perfectly with what we know of the Stoic theory of propositions, and reveals an unsuspected sophistication of Greek mathematics in combinatorial calculation. Hipparchus (circa 190–126 B.C.) was perhaps the greatest astronomer of antiquity. He was an excellent mathematician, and this amazingly sophisticated calculation can only increase our admiration for his accomplishments. For more on the history of the problem, and many other details, the reader should read the delightful article of Stanley [52], as well as the informative analysis of Acerbi [1].

Considerable light has been shed on Plutarch's second number by the discovery of Laurent Habsieger, Maxim Kazarian and Sergei Lando that $(s(10) + s(11))/2 = 310,954$. In their article reporting this observation [14], they give a plausible reading of the notion of negative proposition that leads to this number. The discrepancy of 2 remains unexplained, though Acerbi [1, p. 475] thinks a scribal error is the most probable hypothesis.

The present paper, however, is not concerned with the ancient concept of proposition, but rather with a problem that was first stated in the nineteenth century by William Stanley Jevons. Starting with n propositional variables, there are of course 2^{2^n} logically distinct formulas in classical logic; or in other words, this is the number of distinct Boolean functions in n variables. However, from a more abstract or structural viewpoint, there are fewer functions, since we can regard $p \vee (q \wedge r)$ and $q \vee (p \wedge r)$ as simply two different ways of representing the same three-place function. Furthermore, since it is arbitrary whether we choose p or its negative $\overline{p}$ to represent a proposition, we can also consider $\overline{r} \vee (p \wedge \overline{q})$ as another way of representing the same function. In other words, we consider two Boolean functions to be of the same type if we can obtain one from the other by permuting and complementing variables. How many types of functions are there in n variables? This is Jevons's problem.

Although Jevons's problem was solved in the twentieth century, contemporary logicians do not seem to be well acquainted with it (unlike their nineteenth century predecessors). This lack of knowledge is illustrated by the fact that the problem for four variables was proposed as a logical challenge to promote the Workshop on Logic, Language, Information and Computation (WoLLIC 2005) held on July 19–22, 2005 in Florianópolis, Brazil (the prize was a free copy of the proceedings).

The first part of the paper is devoted to an account of the solution of this problem. The solution is essentially due to George Pólya [40], but we also make use of the work of Palmer and Robinson [37]. The second part recounts the history of the problem. The translations from Pólya's French are by the author. The computer algebra calculations were performed by the open source program Maxima. The author wishes to express his thanks to the referee, whose comments improved the paper substantially.

§2. Enumeration under group action.

2.1. Group theoretic preliminaries. Our group-theoretic notation is mostly adapted from Palmer and Robinson [37]. For general background in permutation groups and combinatorics, see [7] and [27].

If Ω is a finite set, $|\Omega| = m$, then the set of all permutations of Ω forms a group $\mathrm{Sym}(\Omega)$ under the operation of composition; this is the *symmetric group* S_m. A *permutation group* G on Ω is a subgroup of the symmetric group on Ω; the *order* of G, written $|G|$, is the number of permutations in G, and the *degree* of G is $|\Omega| = m$. For G a group, and S a set, an *action* of G on S is a group homomorphism from G into $\mathrm{Sym}(S)$.

If G is a permutation group on Ω, and α a permutation in G, we denote by $j_k(\alpha)$ the number of cycles of length k in the disjoint cycle decomposition of α. The *cycle type* $Z(\alpha)$ is the monomial in the variables $a_1, a_2, \ldots, a_m$ defined by $Z(\alpha) = \prod_{k=1}^{m} a_k^{j_k(\alpha)}$. The *cycle index* $Z(G)$ is the polynomial defined by

$$Z(G) = \frac{1}{|G|} \sum_{\alpha \in G} Z(\alpha).$$

Let G be a permutation group on the set X, and H a permutation group on Y. The *wreath product* $G[H]$ of G and H is defined as follows. The domain of $G[H]$ is the set

$$G \times H^X = \{(g, \phi) \mid g \in G,\ \phi\colon X \to H\},$$

while the group composition is given by $(h, \psi)(g, \phi) = (hg, \theta)$, where θ is defined by $\theta(y) = \psi_{gx}\phi_x(y)$, for $y \in X$. With this definition, $G[H]$ forms a group of order $|G| \cdot |H|^{|X|}$.

The wreath product has a natural action on the set $X \times Y$; for $(g, \phi) \in G[H]$, the permutation defined by (g, ϕ) is given by

$$(g, \phi)(x, y) = (gx, \phi_x(y)).$$

This action can be lifted to an action of $G[H]$ on the set of functions Y^X; the action of (g, ϕ) on the function f is defined by

$$\{(g, \phi)[f]\}(x) = \phi_x(fg^{-1}(x)).$$

The permutation group on Y^X induced by this action of $G[H]$ is the *exponentiation group* $[H]^G$, first defined by Frank Harary [16]. The permutation group $[S_2]^{S_n}$ is the group underlying Jevons's problem, outlined at the end of §1.

2.2. Pólya's theorem. The key to solving Jevons's problem (as well as many other problems in combinatorial enumeration) is a remarkable theorem proved by George Pólya in the 1930s. Pólya's original proof is to be found in his long article [39], which also contains numerous applications to group theory, graph theory and enumeration of chemical compounds. An English translation, together with a history of the theorem and its generalizations can be found in [42]. In this section, we provide a statement of this basic theorem, mostly following the terminology of de Bruijn [10], an adaptation of Pólya's original terminology.

Let D and R be finite sets; we consider functions defined on D taking values in R. Furthermore, we assume given a group G acting on D. The action of G on D induces an action on the set R^D of all functions from D into R; the functions f_1 and f_2 are *equivalent with respect to* G, written $f_1 \sim f_2$, if there is an element $g \in G$ so that $f_1(gd) = f_2(d)$, for all $d \in D$. It is straightforward to check that $\sim$ is an equivalence relation on R^D. The equivalence classes induced by $\sim$ we call *patterns*.

We assume in addition that the elements of R are assigned *weights* $w(r)$; the function w takes values in a commutative ring. If f is a function in R^D, then the weight of f is defined to be

$$W(f) = \prod_{d \in D} w[f(d)].$$

Since multiplication of weights is commutative, it follows that if $f_1 \sim f_2$, then $W(f_1) = W(f_2)$. Hence, we can define the weight $W(F)$ of a pattern F as the weight $W(f)$ of any $f \in F$.

If R is a weighted set with weight function w, we define the *inventory of* R to be $|R|_w = \sum_{r \in R} w(r)$. Hence, if G is a group acting on D, then the *pattern inventory* is $\sum_F W(F)$, where the summation is over the set of all patterns in R^D induced by G. With these definitions, we can now state Pólya's fundamental theorem.

THEOREM 2.1. *Let G be a group acting on a finite set D, R a weighted set, and $Z(G) = Z_G(x_1, x_2, x_3, \ldots)$ the cycle index of the permutation group induced by G on D. Then the pattern inventory resulting from G, D and R is*

$$\begin{aligned}\sum_F W(F) &= Z_G\left[\sum_{r \in R} w(r), \sum_{r \in R}[w(r)]^2, \sum_{r \in R}[w(r)]^3, \ldots\right] \\ &= Z_G[|R|_w, |R|_{w^2}, |R|_{w^3}, \ldots].\end{aligned}$$

COROLLARY 2.2. *The total number of patterns resulting from G, D and R is*

$$Z_G[|R|, |R|, |R|, \ldots].$$

There are numerous expositions of Pólya's theorem in the literature. Pólya's original paper [39, 42] is still very much worth reading, as is the survey of de Bruijn [10]. More recent expositions can be found in [6], [3], and [2]. Kerber's monograph [27] contains a very detailed exposition of the theorem and related results, as well as a good deal of the group-theoretical background. The corollary follows immediately from the theorem, by defining the weight of all elements of R to be 1.

§3. Pólya's solution of Jevons's problem.

3.1. Boolean functions and the exponentiation group. Jevons first stated his problem in the 1870s. He himself solved the problem, essentially by a brute-force approach, only in the case of two and three variables. Clifford extended his solution to four variables, though his solution contains some errors. We describe the early history of the problem below, in the historical part of this paper.

George Pólya was the first to give a systematic and efficient means of solving the problem in his paper of 1940, as an application of his theorem on enumeration. To apply Theorem 2.1, we take D to be the set of all n-vectors of truth-values, $D = \{\top, \bot\}^n$, and R to be the set of truth-values $\{\top, \bot\}$. In addition, let us assume that the weight function w takes values in the ring of polynomials in a single variable x, and define $w(\top) = x$, $w(\bot) = 1$. Then the weight $W(f)$ of a Boolean function indicates the number of inputs on which it takes the value $\top$; that is, if f takes the value $\top$ on k inputs, then $W(f) = x^k$.

Pólya gives a very clear exposition of how his theorem solves Jevons's problem, as well as an illuminating view of the problem in terms of colouring the vertices of an n-dimensional hypercube. However, his paper contains a major lacuna, in that he fails to explain a crucial point, namely, how to compute the cycle index of the appropriate permutation group. In the following subsections, we attempt to fill this lacuna, and give a detailed calculation for the case of four variables.

If our Boolean functions contain n variables, then the permutation group representing permutations of the set of variables is the symmetric group S_n. The complementation group acting on the set of truth values $\{\top, \bot\}$ is the symmetric group S_2. Consequently, the group corresponding to both variable permutations and complementation is the wreath product $S_n[S_2]$. As we noted above in §2.1, there are two natural actions associated with this group. If we consider the action of $S_n[S_2]$ on $\{p_1, \dots, p_n\} \times \{\top, \bot\}$, then the group acts on the set of literals (variables and their negations), where we identify $p_i = (p_i, \top)$ and $\overline{p_i} = (p_i, \bot)$.

However, this is not the action that is crucial in solving Jevons's problem; the appropriate action is on $\{\top, \bot\}^{\{p_1,\dots,p_n\}}$ resulting in the exponentiation group $[S_2]^{S_n}$. The cycle index resulting from the action on $\{p_1, \dots, p_n\} \times \{\top, \bot\}$ is relatively easy to compute, and in fact, Pólya's original paper [39] contains the computation of the cycle index of the action of $G[H]$ on the set $X \times Y$ as an application of his enumeration theorem—de Bruijn also provides a direct computation of the cycle index in his survey paper [10]. The computation of the cycle index of the exponentiation group is a more complex problem. Pólya [40] computes this cycle index for $n = 1, 2, 3, 4$, but does not indicate how he did it, confining himself to the somewhat cryptic remarks:

For a given n, it is only a question of patience to construct the cycle index by computing the $n!2^n$ permutations and their cycle decomposition. I have carried out this calculation for $n = 1, 2, 3, 4$. In carrying it out, numerous simplifications can be found that I do not mention here. I give my results in two tables [40, pp. 101–102].

3.2. The cycle index of the exponentiation group. The cycle index of the exponentiation group $[S_2]^{S_n}$ has been computed in the literature, by Slepian [49] and Harrison [18]. Here, we derive it as a consequence of a general result of Palmer and Robinson [37].

Palmer and Robinson's theorem expresses the cycle index of $[H]^G$ in terms of the cycle indices of G and H. Let G be a group of permutations of $X = \{1, 2, \ldots, m\}$, and H a group of permutations of $Y = \{1, 2, ..., n\}$, and let $Z(G)$ and $Z(H)$ be their respective cycle indices. To express the cycle index of $[H]^G$ in terms of $Z(G)$ and $Z(H)$, we perform a relatively complicated substitution in $Z(G)$. The next few definitions are preliminaries to the description of this substitution.

Let $\mathbf{R} = \mathbf{Q}[b_1, b_2, \ldots]$ be the ring of polynomials in the commuting variables $b_1, b_2, \ldots$ over the ring $\mathbf{Q}$ of rational numbers. We define a multiplication operation on $\mathbf{R}$, first introduced by Harary [15]. For two monomials in $\mathbf{R}$, we define

$$b_1^{i_1} b_2^{i_2} \ldots b_k^{i_k} \times b_1^{j_1} b_2^{j_2} \ldots b_l^{j_l} = \prod_{s=1}^{k} \prod_{s=1}^{l} b_{[s,t]}^{(s,t) i_s j_t}, \tag{1}$$

where $[s, t]$ and (s, t) denote the l.c.m. and g.c.d. of s and t. Then $\times$ is the unique $\mathbf{Q}$-bilinear operation on $\mathbf{R}$ satisfying (1). It is not hard to check that $\times$ is associative.

If S is any non-empty set, we define operations of scalar multiplication over $\mathbf{Q}$, multiplication and addition for elements of $\mathbf{R}^S$ as follows. For $f, g \in \mathbf{R}^S$, $\lambda \in \mathbf{Q}$ and P in S:

$$(\lambda f)P = \lambda(fP), \tag{2}$$

$$(f + g)P = fP + gP, \tag{3}$$

$$(fg)P = fP \times gP. \tag{4}$$

These defined operations make $\mathbf{R}^S$ into a commutative ring over $\mathbf{Q}$, denoted by $S(+, \times)$.

For r a positive integer, define the operator I_r to be the unique $\mathbf{Q}$-linear element of $\mathbf{R}(+, \times)$ satisfying

$$I_r \left(\prod_{k=1}^{n} b_k^{j_k} \right) = \prod_{v=1}^{n^r} b_v^{i_v} \tag{5}$$

where $n = |Y|$ is the degree of the permutation group H, and i_v is defined by

$$i_v = \frac{1}{v} \sum_{w|v} \mu\left(\frac{v}{w}\right) \left(\sum k j_k\right)^{(r,w)}, \tag{6}$$

where the inner sum is taken over all divisors k of $w/(r,w)$, and μ is the Möbius function.

With these preparations completed, we can now state the main theorem of Palmer and Robinson [37].

THEOREM 3.1. *The cycle index of* $[H]^G$ *is obtained by substituting the operators* I_r *for the variables* $b_1, b_2, \ldots, b_r, \ldots$ *in* $Z(G) = Z_G(b_1, b_2, \ldots, b_r, \ldots)$, *and then applying the resulting operator to* $Z(H)$. *That is to say,*

$$Z([H]^G) = Z_G(I_1, I_2, \ldots, I_r, \ldots)[Z(H)].$$

3.3. The cycle index of $[S_2]^{S_n}$**.** In the present section, Theorem 3.1 is applied to compute the cycle index of $[S_2]^{S_n}$. The wreath product $S_n[S_2]$ is the group of symmetries of the n-dimensional hypercube—alternatively (since the hypercube and hyperoctahedron are dual polyhedra), the n-dimensional hyperoctahedron, giving rise to the name “hyperoctahedral group” [55].

The computation begins with the cycle indices of the symmetric groups S_n and S_2. These are easily found from the well known formula

$$Z(S_n) = \sum_{(j)} \prod_{k=1}^{n} \frac{1}{j_k!} \left(\frac{a_k}{k}\right)^{j_k},$$

where the subscript j ranges over n-tuples of non-negative integers $j = (j_1, \ldots, j_n)$ satisfying the equation $1j_i + 2j_2 + \cdots + nj_n = n$. A table of the cycle indices of $Z(S_n)$ for $n \leq 10$ can be found in the book of Harary and Palmer [17, Appendix III].

In its general form, Theorem 3.1 is rather complicated; in particular, the nature of the operators I_r is not easy to understand. However, in the present application, our task is made considerably easier by the fact that we only need to compute I_r for two monomials. The cycle index of S_2 is

$$Z(S_2) = \frac{1}{2}(a_1^2 + a_2),$$

so that we only need to compute $I_r(a_1^2)$ and $I_r(a_2)$, for any r.

For $m = 0, 1, 2, 3, \ldots$, define the function $e(m)$ by

$$e(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) 2^d.$$

The function $e(m)$ appears in numerous combinatorial contexts. The number of degree m irreducible polynomials over $GF(2)$ is $e(m)$; it is also the number of binary Lyndon words of length m [31, §5.1]. For further appearances of the function, the reader can consult the *Encyclopedia of Integer Sequences* [50], where it appears as sequence M0116; the on-line version of the Encyclopedia (where it is sequence A001037) contains many more references. The values of e for $m = 0, 1, 2, \ldots, 12$ are easily computed as $1, 2, 1, 2, 3, 6, 9, 18, 30, 56, 99, 186$.

LEMMA 3.2.

$$I_r(a_1^2) = \prod_{v|r} a_v^{e(v)}.$$

PROOF. The Lemma amounts to showing that if $v|r$, then $i_v = e(v)$, and if $v \nmid r$, then $i_v = 0$. For the first part, let us assume that $v|r$. Then

$$i_v = \frac{1}{v} \sum_{w|v} \mu\left(\frac{v}{w}\right) 2^{(r,w)} \tag{7}$$

$$= \frac{1}{v} \sum_{w|v} \mu\left(\frac{v}{w}\right) 2^{w} = e(v), \tag{8}$$

since $w|v|r$. For the second part, assume that $v \nmid r$. Then for some prime p, and $\alpha > 0$, $v = p^\alpha s$, $p \nmid s$, and $p^\alpha \nmid r$. Hence,

$$i_v = \frac{1}{v} \sum_{w|v} \mu\left(\frac{v}{w}\right) 2^{(r,w)} \tag{9}$$

$$= \frac{1}{v} \sum_{u|s} \left[\mu\left(\frac{v}{p^\alpha u}\right) 2^{(r,p^\alpha u)} + \mu\left(\frac{v}{p^{\alpha-1} u}\right) 2^{(r,p^{\alpha-1} u)}\right] \tag{10}$$

$$= \frac{1}{v} \sum_{u|s} \left[\mu\left(\frac{s}{u}\right) 2^{(r,p^\alpha u)} + \mu\left(\frac{sp}{u}\right) 2^{(r,p^{\alpha-1} u)}\right] \tag{11}$$

$$= \frac{1}{v} \sum_{u|s} \left[\mu\left(\frac{s}{u}\right) 2^{(r,p^\alpha u)} + \mu\left(\frac{s}{u}\right) \mu(p) 2^{(r,p^{\alpha-1} u)}\right] \tag{12}$$

$$= 0. \tag{13}$$

Equation (10) follows because $\mu(p^2) = 0$, equation (13) because $p^\alpha \nmid r$. ⊣

To compute $I_r(a_2)$, we again define an auxiliary function. The function $g(k)$, for $k = 0, 2, 4, 6, 8, \ldots$ is defined by

$$g(2m) = \frac{1}{2m} \sum_{d|2m,\ d\nmid m} \mu\left(\frac{2m}{d}\right) 2^{d/2},$$

while $g(k) = 0$, for k odd. If we ignore the odd values of g, by defining $h(n) = g(2n)$, then we find that the sequence $h(0), h(1), h(2), \ldots$ occurs frequently in the literature of number theory and combinatorics. The number of self-reciprocal polynomials of degree n over $GF(2)$ is $h(n)$; it is also the number of n-bead necklaces with beads of two colours and primitive period n, where turning over is not allowed, but the two colours can be interchanged. For other manifestations of $h(n)$, the reader can consult the *On-Line Encyclopedia of Integer Sequences*, where it is listed as sequence A000048 [50, M0711].

LEMMA 3.3.

$$I_r(a_2) = \prod_{v|2r,\ v\nmid r} a_v^{g(v)}.$$

PROOF. We begin by observing that the condition $v|2r,\ v \nmid r$ is equivalent to the condition $v/(r,v) = 2$, and that by equation (6), we have

$$i_v = \frac{1}{v}\sum_{w} \mu\left(\frac{v}{w}\right) 2^{(r,w)},$$

where the summation is over all divisors w of v, where $w/(r,w)$ is even. The proof of the Lemma is in two parts. In the first part, we show that if $v/(r,v) = 2$, then $i_v = g(v)$; in the second, we show that if $v/(r,v) \neq 2$, then $i_v = 0$.

For the first part, assume that $v/(r,v) = 2$. Since v is even, we can write $v = 2m$. Then if $w|v$, and $w/(r,w)$ is even, then $w/(m,w) = 2$, showing that $i_v = g(v)$.

For the second part, assume that $v/(r,v) \neq 2$. If $v/(r,v)$ is odd, and $w|v$, then $w/(r,w)$ is also odd, showing that $i_v = 0$. So, we can assume that $v/(r,v)$ is even. There are two subcases to consider.

First, let us assume that $v/(r,v)$ is divisible by 4. Thus, we can express v and r in the form $v = 2^{\alpha}s$, $r = 2^{\beta}t$, where $2 \nmid s$, $2 \nmid t$, and $\alpha - \beta \geq 2$. If $w|v$ and $\mu(v/w) \neq 0$, then either $w = 2^{\alpha}u$, or $w = 2^{\alpha-1}u$, where $u|s$, $2 \nmid u$. In either case, $w/(r,w)$ is even, so we have

$$\begin{aligned} i_v &= \frac{1}{v}\sum_{u|s}\left[\mu\left(\frac{v}{2^{\alpha}u}\right)2^{(r,2^{\alpha}u)} + \mu\left(\frac{v}{2^{\alpha-1}u}\right)2^{(r,2^{\alpha-1}u)}\right] && (14)\\ &= \frac{1}{v}\sum_{u|s}\left[\mu\left(\frac{s}{u}\right)2^{(r,2^{\alpha}u)} + \mu\left(\frac{s}{u}\right)\mu(2)2^{(r,2^{\alpha-1}u)}\right] && (15)\\ &= 0, && (16) \end{aligned}$$

where equation (16) follows because $(r, 2^{\alpha}u) = 2^{\beta}(t,u) = (r, 2^{\alpha-1}u)$.

Second, let us suppose that $v = 2^{\alpha+1}s$, $r = 2^{\alpha}t$, where $s \nmid t$, $2 \nmid s$, and $2 \nmid t$. Hence, there is a prime $p > 2$ so that for some β, $p^{\beta}|s$, $p^{\beta} \nmid t$, where $p \nmid s/p^{\beta}$. If $w|v$, and $w/(r,w)$ is even, then $w = 2^{\alpha+1}u$, where $u|s$. It follows that if $\mu(v/w) \neq 0$, then $w = 2^{\alpha+1}p^{\beta}q$, or $w = 2^{\alpha+1}p^{\beta-1}q$, where $p^{\beta}q|s$, and $p \nmid q$. Hence, writing g for $2^{\alpha+1}p^{\beta}$,

$$i_v = \frac{1}{v}\sum_{q|s}\left[\mu\left(\frac{v}{gq}\right)2^{(r,gq)} + \mu\left(\frac{vp}{gq}\right)2^{(r,gq/p)}\right] \tag{17}$$

$$= \frac{1}{v}\sum_{q|s}\left[\mu\left(\frac{v}{gq}\right)2^{(r,gq)} + \mu\left(\frac{v}{gq}\right)\mu(p)2^{(r,gq/p)}\right] \tag{18}$$

$$= 0, \tag{19}$$

where equation (19) follows from the fact that $p^{\beta} \nmid r$. $\dashv$

We have deduced Lemmas 3.2 and 3.3 by an indirect method. However, it is possible to explain their significance by a more direct combinatorial attack that depends on an analysis of the structure of elements in the wreath product $S_n[S_2]$. An element of this group can be written in the form $\langle\sigma;\tau\rangle$, where τ is a vector of n elements in $\{0,1\}$, for example $\langle(1,3,7)(2,5)(4,6);0100111\rangle$. The vector τ is to be interpreted in terms of elements of S_2, where $h_i(x) = x \oplus \tau_i$ represents an operation on $\{0,1\}$.

In the example above, we can classify the cycles constituting the permutation σ as *even* or *odd*. For example, the first cycle, $(1,3,7)$, is odd, since the corresponding entries in τ, 001, sum to 1 modulo 2. Similarly, the second cycle is even and the third odd. The basic result of Alfred Young's analysis of the hyperoctahedral group in [55] with the product action on $X \times Y$ (the first action described in §2.1) is that the cycle structure of a permutation induced by an element of $S_n[S_2]$ is uniquely determined by its component cycles, together with their classification as even or odd.

If we consider an element of $S_n[S_2]$ in its action on the set of functions Y^X, then the cycle structure of this action is determined by the cycle structure of its action on $X \times Y$. Consequently, Young's analysis of the hyperoctahedral group applies to the analysis of this action as well. The content of our two lemmas can now be explained as follows. Let $\langle\sigma;\tau\rangle$ be an element of the wreath product $S_r[S_2]$, where S_r acts on $X = \{1,\dots,r\}$, and S_2 on $Y = \{0,1\}$, where σ is a cycle of length r. Let ϕ be the permutation on Y^X induced by $\langle\sigma;\tau\rangle$. Then if σ is an even cycle (that is to say, the sum of τ modulo 2 is even), the cycle structure of ϕ is $I_r(a_1^2) = \prod_{v|r} a_v^{e(v)}$, while if it is an odd cycle, the cycle structure of ϕ is $I_r(a_2) = \prod_{v|2r,\ v\nmid r} a_v^{g(v)}$; this explains the combinatorial significance of the two lemmas.

The two lemmas only apply to the case where σ consists of a single cycle. However, the operation $\times$ on monomials defined by (1) allows the extension of the computation to arbitrary permutations σ. The direct combinatorial analysis outlined above is the method employed by Slepian [49] and Harrison [18], [20, Chapter 5].

Theorem 3.1 can be combined with Lemmas 3.2 and 3.3 to produce a single formula for the cycle index of $[S_2]^{S_n}$, given by Harrison [18, p. 826], [20, §5.9, Theorem 3]. In the next subsection, we illustrate the results of this section by computing the number of types of Boolean functions in four variables. The computation for three variables can be found in the paper of Palmer and Robinson [37, p. 127].

3.4. Boolean function types in four variables. The computation starts with the cycle index of the symmetric group of degree four:

$$Z(S_4) = \frac{1}{24}[a_1^4 + 6a_1^2 a_2 + 8a_1 a_3 + 3a_2^2 + 6a_4].$$

The next step is to convert the cycle index into the corresponding operator on the ring **R** of polynomials, with the result:

$$\frac{1}{24}[I_1^4 + 6I_1^2 I_2 + 8I_1 I_3 + 3I_2^2 + 6I_4]. \tag{20}$$

The terms of (20) act on $Z(S_2)$ in accordance with equation (4), so that

$$I_1^4(Z(S_2)) = I_1(Z(S_2)) \times I_1(Z(S_2)) \times I_1(Z(S_2)) \times I_1(Z(S_2)), \tag{21}$$

$$\{I_1^2 I_2\}(Z(S_2)) = I_1(Z(S_2)) \times I_1(Z(S_2)) \times I_2(Z(S_2)), \tag{22}$$

$$\{I_1 I_3\}(Z(S_2)) = I_1(Z(S_2)) \times I_3(Z(S_2)), \tag{23}$$

$$I_2^2(Z(S_2)) = I_2(Z(S_2)) \times I_2(Z(S_2)). \tag{24}$$

Employing Lemmas 3.2 and 3.3, we can compute

$$\begin{aligned}
I_1(Z(S_2)) &= Z(S_2) = \frac{(b_1^2 + b_2)}{2}, \\
I_2(Z(S_2)) &= \frac{(I_2(b_1^2) + I_2(b_2))}{2} \\
&= \frac{(b_1^2 b_2 + b_4)}{2}, \\
I_3(Z(S_2)) &= \frac{(I_3(b_1^2) + I_3(b_2))}{2} \\
&= \frac{(b_1^2 b_3^2 + b_2 b_6)}{2}, \\
I_4(Z(S_2)) &= \frac{(I_4(b_1^2) + I_4(b_2))}{2} \\
&= \frac{(b_1^2 b_2 b_4^3 + b_8^2)}{2}.
\end{aligned}$$

Hence, using (21), (22), (23), (24), and the definition of $\times$, we find

$$\begin{aligned}
I_1^4(Z(S_2)) &= (b_1^{16} + 15b_2^8)/16, \\
\{I_1^2 I_2\}(Z(S_2)) &= (b_1^8 b_2^4 + 3b_2^8 + 4b_4^4)/8, \\
\{I_1 I_3\}(Z(S_2)) &= (b_1^4 b_3^4 + 3b_2^2 b_6^2)/4, \\
I_2^2(Z(S_2)) &= (b_1^4 b_2^6 + 3b_4^4)/4.
\end{aligned}$$

$k\backslash n$	1	2	3	4	5
0	1	1	1	1	1
1	1	1	1	1	1
2	1	2	3	4	5
3		1	3	6	10
4		1	6	19	47
5			3	27	131
6			3	50	472
7			1	56	1,326
8			1	74	3,779
9				56	9,013
10				50	19,963
11				27	38,073
12				19	65,664
13				6	98,804
14				4	133,576
15				1	158,658
16				1	169,112
T_n	3	6	22	402	1,228,158

TABLE 1. Table of the numbers $N_n^{(k)}$ for $n = 1, \dots, 5$.

We can now extend these results by linearity to find the image of $Z(S_2)$ under the operator (20):

$$Z([S_2]^{S_4}) = \frac{1}{24}\left[\frac{(b_1^{16} + 15b_2^8)}{16} + 6\frac{(b_1^8 b_2^4 + 3b_2^8 + 4b_4^4)}{8} + 8\frac{(b_1^4 b_3^4 + 3b_2^2 b_6^2)}{4} \right.$$
$$\left. + 3\frac{(b_1^4 b_2^6 + 3b_4^4)}{4} + 6\frac{(b_1^2 b_2 b_4^3 + b_8^2)}{2}\right] \tag{25}$$
$$= \frac{1}{384}\left[b_1^{16} + 51b_2^8 + 12b_1^8 b_2^4 + 84b_4^4 + 32b_1^4 b_3^4 + 96b_2^2 b_6^2 \right.$$
$$\left. + 12b_1^4 b_2^6 + 48b_1^2 b_2 b_4^3 + 48b_8^2\right]. \tag{26}$$

Equation (25) is essentially the same as that given in [40], so we seem to have succeeded in retracing George Pólya's hidden footsteps.

Finally, we can enumerate the types of Boolean functions in four variables, by substituting $1 + x^k$ for b_k in the cycle index $Z([S_2]^{S_4})$. The result is

$$Z([S_2]^{S_4})[b_k := 1 + x^k] = x^{16} + x^{15} + 4x^{14} + 6x^{13} + 19x^{12} + 27x^{11}$$
$$+ 50x^{10} + 56x^9 + 74x^8 + 56x^7 + 50x^6 + 27x^5$$
$$+ 19x^4 + 6x^3 + 4x^2 + x + 1. \tag{27}$$

Equation (27) tells us, for example, that there are 50 types of Boolean function in four variables that take the value $\top$ on 10 inputs. If we substitute 1 throughout for x in (27) (or, alternatively, substitute 2 directly for all the variables in equation (26)), we find that there are 402 types of Boolean functions in four variables, in agreement with the results of Pólya [40].

The algorithm of this section may seem fairly intricate. However, with a little practice, the calculations can be done fairly efficiently, even by hand. It is possible to enumerate the 1,228,158 types of Boolean functions in 5 variables in a few hours, using only pen and paper together with a computer algebra system to perform the final expansion. Table 1 shows the values of $N_n^{(k)}$ for $n = 1, \ldots, 5$—the remaining 16 values for $n = 5$ can be filled in by symmetry. More extensive tables can be found in the work of Harrison [18, p. 827] [20, p. 150].

§4. The history of the problem.

4.1. Jevons and inductive inference. The system that we call "Boolean algebra" might with more justice be called "Jevons algebra"—or perhaps "Jevons-Venn algebra," to give equal billing to Jevons's great rival,[1] John Venn. Whereas Boole's original system contains aspects that are quite strange and unfamiliar to contemporary logicians, the work of Jevons, in spite of some oddities, is easily recognized as an ancestor of current logical ideas.

Jevons followed traditional logical practice in developing a logic of terms, rather than a logic of propositions. He employs capital letters $A, B, C, \ldots$ to stand for adjectival or substantive nouns ("iron", "metal", etc.), while the corresponding lower case letters $a, b, c, \ldots$ stand for the corresponding negative terms ("non-iron", "non-metal", etc.) [23]. He lays great stress on the equational rule of substitution of equals as the sole rule of inference, and shows how the traditional syllogistic logic can be reduced to calculations with this rule. Conjunction of terms is indicated by juxtaposition, so that, for example, the proposition "All metals are conductors" can be symbolized by an equation of the form $AB = A$. In addition, Jevons deploys the symbol $\cdot|\cdot$ for inclusive disjunction.

Jevons's choice of notation led him in a natural way to his problem of enumeration. Jevons followed his teacher Augustus de Morgan by employing a lower-case letter a for the contrary of a term A [11, p. 38]. De Morgan insists strongly on the symmetry between a term and its negation. Consequently, the interchange of A and a appears as a completely natural operation in the context of Jevons's system—more natural than the interchange of p and $\overline{p}$.

[1] "Excellent as much of Jevons' work is,—especially as regards the principles of physical and economical science,—I cannot but hold that in the domain of Logic his inconsistencies and contradictions are remarkable" [54, p. 165].

FIGURE 2. William Stanley Jevons.

His logical rules are the familiar ones of Boolean algebra, with one slight oddity. He insists that his symbols for terms should have non-empty denotations:

> In all probability we ought to assume as a fundamental logical axiom that *every term has its negative in thought*. We cannot think at all without separating what we think about from other different things, and these things necessarily form the negative notion. [23, p. 88]

This quirk of Jevons's logic affects his enumeration of types of propositions, as we shall see below.

Jevons here was again following his teacher, Augustus de Morgan, who in his *Formal Logic* [11, pp. 110–111] remarks:

> On looking into any writer on logic, we shall see that *existence* is claimed for the significations of all the names. Never, in the statement of a proposition, do we find any room left for the alternative *suppose there should be no such things*. Existence as objects, or existence as ideas, is tacitly claimed for the terms of every syllogism.

This conservative attitude towards the question of existential import marks De Morgan and Jevons as transitional figures between traditional and modern logic.

Jevons hit upon his problem as a consequence of his views on inductive inference. His view of induction is that it is simply the inverse of deduction, as subtraction is the inverse of addition.

> Induction is, in fact, the inverse operation to deduction, and cannot be conceived to exist without the corresponding operation, so that the question of relative importance cannot arise. Who thinks of asking whether addition or subtraction is the more important process in arithmetic? [23, p. 139]

Jevons's discussion of inductive inference leads him to a remarkable anticipation of some of the key ideas underlying public key cryptography. He points out that certain functions are easy to compute, while their inverses seem to be intractable:

> Given any two numbers, we may by a simple and infallible process obtain their product, but it is quite another matter when a large number is given to determine its factors. Can the reader say what two numbers multiplied together will produce the number 8,616,460,799? I think it unlikely that any one but myself will ever know; for they are two large prime numbers, and can only be rediscovered by trying in succession a long series of prime divisors until the right one be fallen upon. The work would probably occupy a good computer for many weeks, but it did not occupy me many minutes to multiply the two factors together [23, p. 141].

Of course, Jevons was mistaken about his particular example—anybody equipped with a computer algebra program can discover the two prime factors in hardly more time than it takes to type the number itself. What is more, Jevons's number was factored by hand as early as 1903 by D. N. Lehmer [30]; in a footnote to his paper, Lehmer remarks: "I think that the number has been resolved before, but I do not know by whom." Solomon Golomb succeeded in factoring Jevons's number in less than six minutes, using only a 10-place hand-held calculator, and goes on to say:

> This success led me to consider how easy or difficult it would have been for someone in the 1870's, using only hand calculation, to have succeeded in finding this factorization. I concluded that *at most* a few hours, and quite possibly less than an hour, would have been sufficient! [12]

However, Jevons's mistaken idea about the difficulty of his own example does not affect the striking fact that the problem of factoring the product of two large primes is at the heart of the RSA cryptosystem, used every day in countless transactions over the Internet. The security of this system rests on the assumed intractability of Jevons's factoring problem.

In the context of his logical calculus, Jevons's view of inductive inference amounts to the following problem: given a certain number of terms, such as ABc, aBc etc. representing possible observations, together with certain excluded terms, find a set of equations corresponding to the possible observations. For example, if the only excluded term is Ab, then the corresponding equation is a "partial identity," $A = AB$. Jevons provides what he describes as the "complete solution of the inverse or inductive logical problem" in the case of two terms [23, pp. 154–157]. His solution is that "the laws governing the combinations of two terms must be capable of expression either in a partial identity $(A = AB)$, or a simple identity $(A = B)$" [23, p. 157].

If we think of Jevons's solution in terms of Boolean functions in two variables, then we see that he only considers the functions $A \to B$ and $A \leftrightarrow B$. Functions of the form $\perp$, $A \wedge B$ and A are excluded from the list of "laws governing the combinations of two terms," since they imply the falsity of a one-variable term, contradicting Jevons's view that terms should have non-empty denotations. For example, if we write conjunction in Jevons's notation as the equation $AB = 1$, then this law implies $A = 1$, and hence $a = 0$, contradicting his assumption quoted above.

The omission of the tautology $\top$ simply represents the fact that it is determined by the empty set of equations (Jevons considers including it elsewhere [23, p. 161]).

Jevons also provides a complete solution to his problem of inductive inference in the case of three terms:

> The logical complexity of the problem is so great that the ordinary modes of calculating numbers of combinations in mathematical science fail to give any aid, and exhaustive examination of the combinations in detail is the only method applicable.
>
> My mode of solving the problem was as follows:– Having written out the whole of the 256 series of combinations, I examined them separately and struck out such as did not fulfil the test of consistency. I then chose some common form of proposition involving two or three terms, and varied it in every possible manner, both by the circular interchange of letters $(A, B, C$ into B, C, A and then $C, A, B)$, and by the substitution for any one or more of the terms of the corresponding negative terms. . . . I proceed in this way to work out the results of every form of law which I can find or invent [23, pp. 158–159].

In the quotation above, the "test of consistency" alludes to the fact that Jevons ruled out propositions implying that either A or a is empty, for some term A.

Jevons was pessimistic about this approach by exhaustive enumeration in the case of four variables:

> Some years of continuous labour would be required to ascertain the precise number of types of laws which may govern the combinations of only four things, and but a small part of such laws would be exemplified or capable of practical application in science. The purely logical inverse problem, whereby we pass from combinations to their laws, is solved in the preceding pages, as

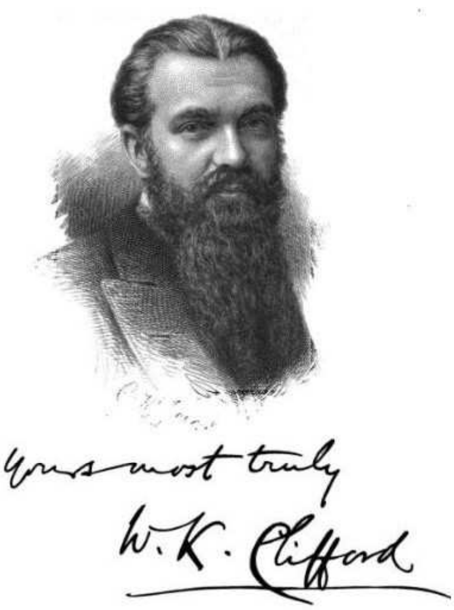

FIGURE 3. William Kingdon Clifford.

> far as it is likely to be for a long time to come; and it is almost impossible that it should ever be carried more than a single step further [23, pp. 163–164].

The implicit challenge in these remarks was shortly taken up by William Kingdon Clifford. In the second edition of his *Principles of Science* (1877), Jevons wrote:

> In the first edition (vol. 1. p. 163), I asserted that some years of labour would be required to ascertain even the precise number of types of law governing the combinations of four classes of things. Though I still believe that some years' labour would be required to work out the types themselves, it is clearly a mistake to suppose that the *numbers* of such types cannot be calculated with a reasonable amount of labour, Professor W. K. Clifford having actually accomplished the task [24, p. 143].

In the next section, we shall examine Clifford's attempted solution of the four variable problem.

4.2. Clifford and the problem of four variables. William Kingdon Clifford, an outstanding geometer whose death from tuberculosis in 1879 at the age of 33 was a great loss to Victorian mathematics, found it hard to resist a mathematical challenge. His editor, Robert Tucker, remarks of his reaction to Jevons's posing of the four variable problem:

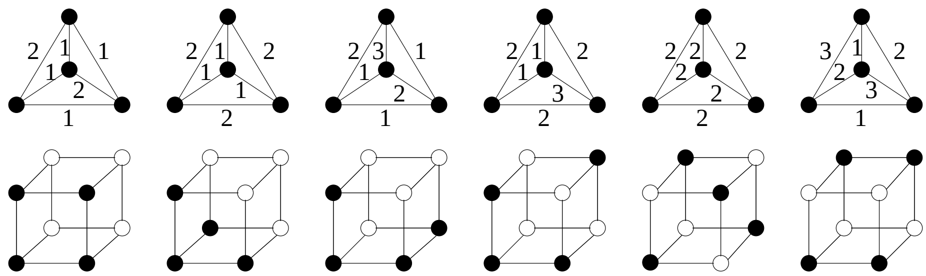

FIGURE 4. Six colouring patterns on the cube, and their labelled graphs.

> It was on reading Prof. Jevons's original statements that Prof. Clifford said laughingly, he couldn't let anyone say that and not do it straight off . . . it was 'his luck' to do quickly difficult things which were usually got at by long processes only [9, p. 16].

H. J. S. Smith wrote of Clifford that he was "above all and before all a geometer" [9, p. xxxvii]. Consequently, it is not surprising to find that Clifford attempted the problem of enumerating types of Boolean functions by an essentially geometrical method [8]. We can think of a Boolean function in n variables as corresponding to a set of vertices in an n-dimensional cube (the vertices being those vectors of truth-values where the function takes the value $\top$). From a geometrical point of view, Jevons's problem amounts to classifying sets of such vertices under the equivalence relation induced by the symmetries of the underlying n-dimensional cube.

It is worth remarking that Clifford simply ignores Jevons's restriction to non-empty terms, not thinking it even worthy of notice. Later algebraic logicians such as C. S. Peirce and Ernst Schröder followed him in this attitude. In fact, Schröder [45, p. 671] finds it surprising that Clifford, while providing a solution for the case of 4 variables, did not correct Jevons's solution for the case of 3 variables, and describes Jevons's restriction to non-empty terms as a "fundamental error."

We can associate a labelled graph with a set of vertices as follows. The universe of the graph is the set of vertices themselves, with an edge joining every pair of distinct points. The edge between two vertices is labelled with the distance between them (that is, the distance is the familiar Hamming distance of information theory). Figure 4 shows the patterns on the 3-dimensional cube corresponding to the six types of Boolean functions with four $\top$ values, together with the corresponding labelled graphs.

The labelled graphs are invariants of the Boolean functions to which they correspond; that is to say, if two functions are equivalent under the symmetry group $[S_2]^{S_n}$, then their corresponding labelled graphs are the same. For two and three variables, the labelled graphs uniquely determine a type of function. Unfortunately, for four and more variables, this correspondence breaks down, as we shall see below, so the labelled graph is not a complete set of invariants for a Boolean function.

We have described Clifford's construction in terms of patterns on the vertices of an n-dimensional cube. Surprisingly, Clifford himself does not use this terminology, though he does use the notion of 'distance' between 'marks,' defined as the number of complementation operations required to go from one mark to the other. We may suspect that Clifford had the n-dimensional interpretation in mind, since he was perfectly familiar with the notion of n-dimensional space, as his other writings show.

It was natural for Clifford to look for a graphical theory of invariants for Boolean functions, since already in 1875 he had introduced a theory of invariants of binary forms based on graph theory [9, Papers 28 and 31]. Clifford was building on earlier graphical work of Cayley and Sylvester, central figures in the nineteenth century theory of invariants. Some of this history, including the connections to graphical notation used in chemistry to represent molecular structure is given an attractive exposition in [5, Chapter 4]. A modern exposition of Clifford's theory can be found in Chapter 7 of Peter J. Olver's monograph on classical invariant theory [34].

For functions in fewer than four variables, it is not hard to see that Clifford's labelled graphs provide a complete set of invariants. Unfortunately, the correspondence breaks down for four variables, as Clifford pointed out [9, p. 4]. In the Boolean algebra with sixteen elements, consider the set consisting of all four atoms as well as the set containing three atoms, together with a co-atom containing all three. These sets are not equivalent under the group $[S_2]^{S_n}$, but their graphs are the same, since the distance between the vertices is in every case 2.

This failure of the labelled graphs to characterize the type of the function to which they correspond is presumably what accounts for the errors in Clifford's enumeration. If, following Pólya, we write $N_n^{(k)}$ for the number of types of functions in n variables that take the value $\top$ for k inputs, then Clifford finds the values $N_4^{(6)} = 47$, $N_4^{(7)} = 55$, $N_4^{(8)} = 78$, whereas the correct values are $N_4^{(6)} = 50$, $N_4^{(7)} = 56$, $N_4^{(8)} = 74$.

It is worth mentioning here that a theory of invariants for Boolean functions has been developed subsequent to the work of Clifford. However, it is not based on Clifford's geometrical ideas, but rather on a discrete analogue of Fourier analysis. Harrison's textbook [20, pp. 155–167] gives an introduction to the theory.

4.3. From Clifford to Pólya. After Clifford's attempted solution to the case of four variables, Jevons's problem was discussed in the literature of algebraic logic. Christine Ladd describes the problem in her 1883 survey [29] of the algebra of logic. John Venn, in his treatise on symbolic logic remarked:

> Jevons considered that it would take several years of continuous labour even to determine the number of possible types of propositions here; and, though Clifford solved this part of the question by showing that there were 396 such types, he still considers that such a period would be required to ascertain what these types actually are. With five terms, the number of possible selections is 4,294,967,295, and the number of types is one which presumably no man will ever determine [54, p. 324].

It seems a little surprising that both Jevons and Venn thought that actually writing down formulas (or sets of equations) for each of the types in 4 variables would take several years, since Clifford provides an explicit description of his types in terms of subsets of the 4-dimensional hypercube.

Ernst Schröder, in the first volume of his treatise on logic, gives a detailed discussion [45, pp. 659–683]; he also introduces for the first time an explicit description of the problem in terms of classifying subsets of the vertices of an n-dimensional cube, for $n \leq 4$. He reproduces Clifford's results for the 4 variable case, but goes on to say that he has himself calculated the numbers $N_4^{(k)}$ only for $k = 0, 1, 2, 3$ [45, pp. 681–682]. He recommends that mathematicians pursue the problem further.

Continuing in the framework of Schröder, A. Nagy [33] computed the number of types $N_n^{(k)}$ for $k = 0, \ldots, 4$, employing Clifford's approach through the associated labelled graphs. Jevons's problem was seen as a central question by researchers in the tradition of algebraic logic, as may be seen from the introductory remarks in Nagy's paper of 1894, in which he describes it as "of especial importance for logic" [33, p. 331]. However, with the near-eclipse of the algebraic tradition in logic, as a result of the success of the logicist tradition of Frege, Peano, Russell and others, the problem seems to have been largely forgotten by mathematical logicians.

The solution of the problem by George Pólya came through an indirect route. The introduction of graphical notation in mathematics, as we mentioned briefly in §4.2, was inspired by contemporary developments in chemistry. Molecular diagrams provided an explanation for the phenomenon of isomeric compounds, molecules that had different properties in spite of having the same atomic composition. Pólya was inspired to prove his basic theorem on enumeration (Theorem 2.1) by earlier work of chemists such as Henze and Blair who were attempting to enumerate certain classes of molecules.

Pólya was a mathematician with a strong interest in the history of mathematics, as well as in the logic of discovery. It is quite likely that he came across the problem in his reading of Jevons's book on logic [24], the first reference cited in his paper of 1940. After the publication of Pólya's paper, however, the problem seemed to sink into oblivion again, and even now the solution does not seem to be widely known among logicians, as we pointed out earlier. The revival of interest in the problem had to wait for the development of digital computers in the mid-twentieth century. It was the electrical engineers and computer scientists, not the logicians, who revived the nineteenth-century tradition of Boolean algebraic logic.

4.4. Computers and circuits. The modern revival of interest in Jevons's problem arose from neither logic nor combinatorics, but from the more practical discipline of electrical engineering and the design of computer circuits. In his MIT Master's thesis, published in 1938 as the paper [46], Claude Shannon proposed Boolean algebra as a mathematical tool for analyzing switching circuits. The basic model is that of circuits composed of relays and switches. In the 1930s and 1940s, massive computers were built with relays as their basic functional elements. According to Thomas Thompson's entertaining and informative mathematical history,

> The Model V, the penultimate relay computer to be built by Bell, was the largest in the series. Containing over nine thousand relays and over fifty pieces of teletype apparatus, it occupied about one thousand square feet of floor space and weighed some ten tons [53, p. 16].

Clearly, there was a strong economic incentive for building circuits that contained as few relays as possible—hence, Shannon's idea of using Boolean algebra as a tool for circuit simplification.

Shannon followed up his original paper of 1938 with another very influential article of 1949 [47] that provided the basis for the modern theory of circuit complexity. Together with his Master's thesis, this paper is the foundation of all subsequent work in the area. Shannon proves a universal upper bound of $2^{n+3}/n$ on the size of circuits computing Boolean functions in n variables, based on an ingenious construction. Even more significantly, he shows a lower bound that comes close to matching his upper bound; for $\varepsilon > 0$, and sufficiently large n, almost all Boolean functions in n variables require at least $(1 - \varepsilon)2^n/n$ circuit elements. Interestingly, the lower bound is a pure existence proof, proved by a clever but surprisingly simple counting argument.

In the last part of his paper, Shannon remarks that although almost all Boolean functions require exponentially large circuits, the circuits encountered in practice do not seem to require such resources: "In fact, almost all relays encountered in practice have less than 20 elements" [48, p. 618]. He goes on to explain this in terms of certain features of the circuits used in applications. One of these features is symmetry—functions used in practice often have non-trivial symmetries under the group of permutations and complementations.

Shannon's theme of symmetries of functions was taken up again by David Slepian, in a sequel to Pólya's paper, published in 1953 [49]. Like Shannon, Slepian was working at the time in Bell Telephone Laboratories. He describes the synthesis problem as follows:

> Specifying the function f determines the synthesis problem and under suitable restrictions leads to the synthesis of a definite physical network to realize f. From a physical point of view, however, it is immaterial how the n input leads are labelled or which of the two states any lead can assume is called zero or one. Therefore any Boolean function that can be obtained from f by permuting and (or) complementing one or more variables must be regarded as corresponding to the same physical network as f [49, p. 185].

The problem of building a circuit, preferably the simplest possible, is the "synthesis problem" of Shannon and Slepian. It is of course in essence the same as the inductive inference problem of Jevons, so it is not surprising that the modern electrical engineers followed the same paths as their Victorian ancestor.

Slepian followed the same methods as those already used by Pólya, but also supplied the missing ingredient in Pólya's proof, a computation of the cycle index of $[S_2]^{S_n}$. This computation, following the lines that we outlined at the end of §3.3, uses group character theory, together with the work of Alfred Young [55] on the representation theory of the hyperoctahedral group. Slepian computes the number of types of Boolean functions up to 6 variables, finding that there are 400,507,806,843,728 types in 6 variables. The values for 7 and 8 variables can be found in the *On-line Encyclopedia of Integer Sequences* (A000616).

Although relays had been supplanted by vacuum tubes, and subsequently by transistors, basic circuits in computers in the early 1960s remained relatively large and bulky objects, consisting of individual transistors, resistors and capacitors soldered to circuit boards—a good visual impression of the technology of the period can be obtained from the coffee-table book of Mark Richards and John Alderman [44]—for example, see the illustration of the inner circuits of the Philco 212 on pp. 66–67. Hence, the problem of circuit minimization remained a key problem for computer designers.

In a series of papers [18, 19], as well as in his textbook [20], Michael A. Harrison extended and generalized the results of Pólya and Slepian, computing the number of types under the group of variable permutations and the complementation group, in addition to the group of permutations and complementations. His method for computing the cycle index of $[S_2]^{S_n}$ was very similar to that of Slepian, except that he began from the work of Ore on monomial groups [35], rather than that of Young. When Harrison published his papers of 1963 [18, 19], systematic lists of minimal networks had been produced.

> Slepian [49] solved the general problem posed by Pólya and gave an algorithm for counting the number of equivalence classes for arbitrary n. Since that time, a table of 402 minimal contact networks has been constructed for the Boolean functions of four variables. (An early version of the table is reprinted in the book by Higonnet and Grea [13].) One method of synthesizing a function f of four variables is to find which of the 402 representative functions is equivalent to f. The minimal network is selected from the table and suitably relabelled to realize f [18, p. 808].

Harrison's textbook [20] contains as Appendix 5 a complete list of minimal switching circuits for functions of four variables, worked out by Professor I. Ninomiya. This book remains the best and most detailed source for the solution of Jevons's problem. It is worth remarking that Ninomiya's table of minimal networks completely solves Jevons's problem of inductive inference in four variables, giving the simplest possible form of logical formulas representing each type of function.

4.5. Graphical enumeration. Meanwhile, researchers in combinatorics and graph theory were carrying on a parallel stream of research inspired by Pólya's fundamental theorem. An excellent survey of this work up to the early 1970s is to be found in the book of Harary and Palmer [17]; Harary and Palmer also give a detailed exposition of the remarkable work of J. H. Redfield, whose paper of 1927 [43] not only anticipates the work of Pólya, but already solves many of the basic problems of graphical enumeration. This paper was forgotten and neglected until its rediscovery by the community of graph theorists in the late 1950s.

In his paper of 1940, Pólya remarked

> We have, of course, investigated the problem of the types of compound propositions from the point of view of classical logic; we could pose and resolve the problem, using the same general method, for a logic of three or several truth-values; but, for the moment, I see no interest in this possible generalization [40, p. 102].

Nevertheless, Harrison and High [21], extending the earlier work of Harrison, enumerated various classes of Post functions under the action of several groups. As preparation, they compute the cycle index of $[H]^{S_n}$, where H is an arbitrary finite group.

Palmer and Robinson [37] generalized the work of Harrison and High still further to provide a way of computing the cycle index of $[H]^G$ in terms of the cycle indices of G and H, as we saw above in §3.2. (Adalbert Kerber [25], [26, p. 146] gave another method of computing this cycle index, using the permutation character of $[H]^G$.) They apply their results to problems in graphical enumeration, as well as the enumeration of types of Post functions, already investigated by Harrison and High.

Palmer, in his comments on Pólya's classic paper of 1940 [40], says that the methods of Palmer and Robinson "provided the best available method for enumerating the types of Boolean functions" [41, p. 629]. This seems an appropriate point to bring this historical survey to a close. Although Jevons's problem was first raised in the context of mathematical logic, it has subsequently been largely forgotten by the logical community. However, the problem leads to some interesting and attractive mathematics, and deserves to be better known to logicians.

REFERENCES

[1] F. Acerbi, *On the shoulders of Hipparchus: A reappraisal of ancient Greek combinatorics*, ***Archive for History of Exact Sciences***, vol. 57 (2003), pp. 465–503.

[2] Martin Aigner, ***A course in enumeration***, Graduate Texts in Mathematics, no. 238, Springer-Verlag, 2007.

[3] F. Bergeron, G. Labelle, and P. Leroux, *Combinatorial species and tree-like structures*, ***Encyclopedia of mathematics and its applications***, no. 67, Cambridge University Press, 1998.

[4] Kurt-R. Biermann and Jürgen Mau, *Überprüfung einer frühen Anwendung der Kombinatorik in der Logik*, ***The Journal of Symbolic Logic***, vol. 23 (1958), pp. 129–132.

[5] Norman L. Biggs, E. Keith Lloyd, and Robin J. Wilson, ***Graph theory 1736–1936***, Oxford University Press, 1976.

[6] Peter J. Cameron, ***Combinatorics: Topics, techniques, algorithms***, Cambridge University Press, 1994.

[7] ———, ***Permutation groups***, London Mathematical Society Student Texts, no. 45, Cambridge University Press, 1999.

[8] William Kingdon Clifford, *On the types of compound statement involving four classes*, ***Memoirs of the Literary and Philosophical Society of Manchester, Session 1876–1877***, vol. 16 (1877), pp. 88–101, reprinted as Paper 1 in [9].

[9] ———, ***Mathematical papers***, Macmillan and Co., 1882, edited by Robert Tucker, with an introduction by H. J. Stephen Smith. Reprinted, Chelsea Publishing Company, New York 1968.

[10] N. G. de Bruijn, *Pólya's theory of counting*, ***Applied combinatorial mathematics*** (Edwin F. Beckenbach, editor), John Wiley and Sons, 1964, pp. 144–184.

[11] Augustus De Morgan, ***Formal logic: or, the calculus of inference, necessary and probable***, Taylor and Walton, London, 1847.

[12] Solomon W. Golomb, *On factoring Jevons' number*, ***Cryptologia***, vol. 20 (1996), pp. 243–246.

[13] R. Grea and R. Higonnet, ***Logical design of electrical circuits***, Macmillan Co., New York, 1958.

[14] Laurent Habsieger, Maxim Kazarian, and Sergei Lando, *On the second number of Plutarch*, ***American Mathematical Monthly***, vol. 105 (1998), p. 446.

[15] Frank Harary, *On the number of bi-colored graphs*, ***Pacific Journal of Mathematics***, vol. 8 (1958), pp. 743–755.

[16] ———, *Exponentiation of permutation groups*, ***American Mathematical Monthly***, vol. 66 (1959), pp. 572–575.

[17] Frank Harary and Edgar M. Palmer, ***Graphical enumeration***, Academic Press, New York and London, 1973.

[18] Michael A. Harrison, *The number of transitivity sets of Boolean functions*, ***Journal of the Society for Industrial and Applied Mathematics***, vol. 11 (1963), pp. 806–828.

[19] ———, *On the number of classes of (n, k) switching networks*, ***Journal of the Franklin Institute***, vol. 276 (1963), pp. 313–327.

[20] ———, ***Introduction to switching and automata theory***, McGraw-Hill Book Company, 1965.

[21] MICHAEL A. HARRISON and ROBERT G. HIGH, *On the cycle index of a product of permutation groups*, ***Journal of Combinatorial Theory***, vol. 4 (1968), pp. 277–299.

[22] THOMAS HEATH, ***A history of Greek mathematics***, Clarendon Press, Oxford, 1921, reprinted by Dover Publications, 1981.

[23] W. STANLEY JEVONS, ***The principles of science: A treatise on logic and scientific method***, vol. 1, Macmillan and Co., London, 1874.

[24] ———, ***The principles of science: A treatise on logic and scientific method***, second revised ed., Macmillan and Co., London, 1877.

[25] ADALBERT KERBER, *Der Zykelindex der Exponentialgruppe*, ***Mitteilungen aus dem Mathemematischen Seminar Giessen***, vol. 98 (1973), pp. 5–20.

[26] ———, ***Representations of permutation groups II***, Lecture Notes in Mathematics, no. 495, Springer-Verlag, Berlin and Heidelberg and New York, 1975.

[27] ———, ***Applied finite group actions***, second, revised and expanded ed., Algorithms and Combinatorics, no. 19, Springer-Verlag, 1999.

[28] WILLIAM KNEALE and MARTHA KNEALE, ***The development of logic***, Oxford University Press, 1962.

[29] CHRISTINE LADD, *On the algebra of logic*, (Charles Saunders Peirce, editor), Studies in Logic by Members of the Johns Hopkins University, Little, Brown, and Company, Boston, 1883, pp. 17–71.

[30] D. N. LEHMER, *A theorem in the theory of numbers*, ***Bulletin of the American Mathematical Society***, vol. 13 (1907), pp. 501–502.

[31] M. LOTHAIRE, ***Combinatorics on words***, Cambridge University Press, 1997, corrected reissue of the 1983 edition: *Encyclopedia of Mathematics and its Applications*, vol. 17.

[32] BENSON MATES, ***Stoic logic***, University of California Press, 1953.

[33] A. NAGY, *Über das Jevons-Clifford'sche Problem*, ***Monatshefte für Mathematik und Physik***, vol. 5 (1894), pp. 331– 345.

[34] PETER J. OLVER, ***Classical invariant theory***, London Mathematical Society Student Texts, no. 44, Cambridge University Press, 1999.

[35] OYSTEIN ORE, *Theory of monomial groups*, ***Transactions of the American Mathematical Society***, vol. 51 (1942), pp. 15–64.

[36] ROBERT R. O'TOOLE and RAYMOND E. JENNINGS, *The Megarians and the Stoics*, ***Handbook of the history of logic, volume 1: Greek, Indian and Arabic Logic*** (Dov M. Gabbay and John Woods, editors), Elsevier North Holland, 2004, pp. 397–522.

[37] E. M. PALMER and R. W. ROBINSON, *Enumeration under two representations of the wreath product*, ***Acta Mathematica***, vol. 131 (1973), pp. 123–143.

[38] PLUTARCH, ***Moralia***, vol. XIII, Part II, Harvard University Press, 1976, with an English translation by Harold Cherniss.

[39] GEORGE PÓLYA, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen*, ***Acta Mathematica***, vol. 68 (1937), pp. 145–253, reprinted in [41].

[40] ———, *Sur les types des propositions composées*, ***The Journal of Symbolic Logic***, vol. 5 (1940), pp. 98–103, reprinted in [41].

[41] ———, ***Collected papers, volume IV: Probability; combinatorics; teaching and learning in mathematics***, (Gian-Carlo Rota, editor), The MIT Press, Cambridge, Massachusetts, 1984.

[42] GEORGE PÓLYA and RONALD C. READ, ***Combinatorial enumeration of groups, graphs and chemical compounds***, Springer-Verlag, 1987.

[43] J. H. REDFIELD, *The theory of group-reduced distributions*, ***American Journal of Mathematics***, vol. 49 (1927), pp. 433–455.

[44] MARK RICHARDS and JOHN ALDERMAN, ***Core memory: A visual survey of vintage computers***, Chronicle Books, San Francisco, 2007.

[45] ERNST SCHRÖDER, ***Vorlesungen über die Algebra der Logik*** (***exakte Logik***), vol. I, B. G. Teubner, Leipzig, 1890.

[46] CLAUDE E. SHANNON, *A symbolic analysis of relay and switching circuits*, ***Transactions of the American Institute of Electrical Engineers***, vol. 57 (1938), pp. 713–723, reprinted in [48].

[47] ———, *The synthesis of two-terminal switching circuits*, ***Bell System Technical Journal***, vol. 28 (1949), pp. 59–98, reprinted in [48].

[48] ———, ***Collected papers***, (N. J. A. Sloane and Aaron D. Wyner, editors), IEEE Press, 1993.

[49] DAVID SLEPIAN, *On the number of symmetry types of Boolean functions of n variabless*, ***Canadian Journal of Mathematics***, vol. 5 (1953), pp. 185–193.

[50] N. J. A. SLOANE and SIMON PLOUFFE, ***The encyclopedia of integer sequences***, Academic Press, 1995, a greatly expanded version of the Encyclopedia is available on-line at `http://www.research.att.com/~njas/sequences/`.

[51] RICHARD P. STANLEY, ***Enumerative combinatorics***, vol. 1, Wadsworth and Brooks/Cole, Monterey, California, 1986.

[52] ———, *Hipparchus, Plutarch, Schröder and Hough*, ***American Mathematical Monthly***, vol. 104 (1997), pp. 344–350.

[53] THOMAS M. THOMPSON, ***From error-correcting codes through sphere packings to simple groups***, Carus Mathematical Monographs, no. 21, Mathematical Association of America, 1983.

[54] JOHN VENN, ***Symbolic logic***, second ed., Macmillan, London, 1894, reprinted Chelsea Publishing Company, Bronx, New York, 1971.

[55] ALFRED YOUNG, *On quantitative substitutional analysis* (*fifth paper*), ***Proceedings of the London Mathematical Society***, vol. 31 (1930), pp. 273–288.

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF TORONTO
TORONTO, ONTARIO M5S 3G4, CANADA
E-mail: urquhart@cs.toronto.edu