COMMUTATIVE REGULAR EQUATIONS AND PARIKH'S THEOREM

D. L. PILLING

Parikh's Theorem [1] asserts that the commutative image of a context-free language is a semi-linear event—that is, is regular if considered as an event over a commutative alphabet. But the commutative image of a context-free language generated by a grammar Γ is the same as the language generated by Γ when regarded as defined in terms of an already commuting alphabet. Context-free grammars over a commutative alphabet can be defined as in the non-commutative case—we have disjoint alphabets V_T, V_N of terminal and non-terminal letters, a finite set of productions of the form $A \to \phi$, where A is a letter of V_N and ϕ a word over $V_N \cup V_T$, and an initial letter A_0. We write $uAv \to u\phi v$ whenever $A \to \phi$ is a production and u, v words over $V_N \cup V_T$, and $u \xrightarrow{*} z$ if there is a finite chain of words satisfying

$$u \to v \to w \to \ldots \to y \to z .$$

The language generated by this grammar is then the set of all words w with $A_0 \xrightarrow{*} w$, w a word over V_T. We emphasize that the letters in the alphabets V_N, V_T are to be considered as commuting freely with each other.

It is clear that the language generated by a grammar is the smallest solution of a corresponding system of equations. This is simplest seen in terms of an example—the language generated by the grammar

$$A \to A^3 Ba \qquad A \to AB^2 a \qquad A \to b$$

$$B \to AB^2 \qquad B \to a$$

with $V_N = \{A, B\}$, $V_T = \{a, b\}$, and A the initial letter, is the smallest event X for which there is an event Y satisfying:

$$X = X^3\, Ya + XY^2 a + b$$

$$Y = XY^2 + a$$

Parikh's result is then a theorem about solutions of finite equations over a commutative alphabet. It is therefore a special consequence of the theorem proved here on more general regular equations, which has several other applications [2], and perhaps some independent interest. Functions and expressions are defined for events (i.e., sets of words) over a commutative alphabet just as in the non-commutative case. The regular operations are as usual, i.e., $E+F$ is the union of E and F, $EF = \{ef \mid e \in E, f \in F\}$, $E^* = 1+E+E^2+\ldots$, where 1 is the empty word.

LEMMA. *To any system of inequalities*

$$X_0 \supseteq f_0(X_0, \ldots, X_r, X_{r+1}, \ldots, X_m)$$
$$\cdots$$
$$X_r \supseteq f_r(X_0, \ldots, X_r, X_{r+1}, \ldots, X_m)$$

Received 29 March, 1971; revised 1 February, 1972.

[J. LONDON MATH. SOC. (2), 6 (1973), 663–666]

in which $f_0, \ldots, f_r$ are event functions and $X_{r+1}, \ldots, X_m$ arbitrary events, there corresponds a second system,

$$X_0 \supseteq g_0(X_{r+1}, \ldots, X_m)$$
$$\ldots$$
$$X_r \supseteq g_r(X_{r+1}, \ldots, X_m)$$

in which the g_i are functions independent of $X_{r+1}, \ldots, X_m$. The second system is implied by the first, and is the minimal solution of the first in the sense that if $X_0, \ldots, X_r$ satisfy the second system with equality then they satisfy the first with equality also.

Proof. We define sequences of approximating solutions X_{iN} and g_{iN}, $i = 0, \ldots, r$ by the equations

$$X_{i0} = g_{i0}(X_{r+1}, \ldots, X_m) = 0$$

$$X_{i(N+1)} = g_{i(N+1)}(X_{r+1}, \ldots, X_m) = f_i(X_{0N}, \ldots, X_{rN}, X_{r+1}, \ldots, X_m).$$

Then we define $g_i(X_{r+1}, \ldots, X_m) = \sum g_{iN}(X_{r+1}, \ldots, X_m)$ over all N.

Obviously, if events $X_0, \ldots, X_r$ satisfy the first system, we can prove inductively since regular functions are monotonic that $X_i \supseteq g_{iN}(X_{r+1}, \ldots, X_m)$ for all N and so $X_i \supseteq g_i(X_{r+1}, \ldots, X_m)$. If, however, we *define* X_i as $g_i(X_{r+1}, \ldots, X_m)$, then we have

$$X_i = \sum X_{i(N+1)} = \sum f_i(X_{0N}, \ldots, X_{rN}, X_{r+1}, \ldots, X_m) = f_i(X_0, \ldots, X_r, X_{r+1}, \ldots, X_m)$$

since every word of $f_i(X_0, \ldots, X_r, X_{r+1}, \ldots, X_m)$ is in some summand

$$f_i(X_{0N}, \ldots, X_{rN}, X_{r+1}, \ldots, X_m).$$

This shows that the X_i as defined satisfy the first system. (One also notes that commutativity was not used in the argument so that the result holds for non-commutative events as well.)

The lemma allows us to solve such systems piecemeal—given such a system, we can solve a single equation, treating the other variables as constants. The lemma guarantees this solution to be the minimal one, and we can substitute this partial solution into the remaining equations, thus reducing the complexity of the original system of equations.

THEOREM. *A system of regular equations*

$$\left.\begin{aligned} X_0 &= f_0(X_0, \ldots, X_r, X_{r+1}, \ldots, X_m) \\ &\ldots \\ X_r &= f_r(X_0, \ldots, X_r, X_{r+1}, \ldots, X_m), \end{aligned}\right\} \tag{1}$$

in which the f_i are regular functions of their arguments, has a regular minimal solution—that is, the g_i are regular functions.

Proof. We first consider a single equation

$$X_0 = f_0(X_0, \ldots, X_r, X_{r+1}, \ldots, X_m). \tag{2}$$

Using the associative, distributive and commutative laws for events together with the laws $(E+F)^* = E^*F^*$ and $(E^*F)^* = 1+E^*F^*F$, a simple argument shows that the event $f_0(X_0, \ldots, X_r, X_{r+1}, \ldots, X_m)$ can be expressed as a finite sum of terms of the form

$$(w_1 X_0^{q_1})^* \ldots (w_p X_0^{q_p})^* w X_0^q$$

where (i) $w_1, \ldots, w_p$, w are "words" over the variables $X_1, \ldots, X_r$ and fixed events $X_{r+1}, \ldots, X_m$, and (ii) $q_1, \ldots, q_p, q$ are non-negative integers (see remarks below concerning semi-linear events). We can use the first law to eliminate additions within starred expressions and the second law to eliminate starred expressions within starred expressions. After this, every starred item is a " word " over $X_0, \ldots, X_m$ and the commutative law allows us to express the terms in the above form.

Now (2) can easily be put in the form

$$X_0 = E(X_1, \ldots, X_m) + F(X_0, \ldots, X_m).X_0 \tag{3}$$

where E and F are regular functions—we abbreviate this to

$$X_0 = E + F(X_0).X_0.$$

Since regular functions are monotonic this implies that

$$X_0 \supseteq \{F(E)\}^*.E = G^*E, \text{ say},$$

where $G = F(E)$. We now show that G^*E is in fact a solution of (3) and so is the required minimal solution. If $\phi(X_0, \ldots, X_m)$ is any word in $X_0, \ldots, X_m$ which involves X_0, then using the relation $Y^*Y^* = Y^*$ and the commutative law we have

$$\phi(Y^*Z, X_1, \ldots, X_m) = Y^*.\phi(Z, X_1, \ldots, X_m).$$

Using this we derive

$$E + F(G^*E).G^*E = E + G^*.F(E).E = E + G^*.G.E = G^*E,$$

proving our assertion.

To solve systems containing more than one equation, the lemma allows us the use of this result (for a single equation) as the induction step and the fact that regular functions of regular events are regular enables us to eliminate the variables one by one to obtain the general result.

As an example of the technique, we consider the system of two equations which we discussed earlier where $(X_0, X_1, X_2, X_3) = (Y, X, a, b)$:

$$X = X^3\,Ya + XY^2\,a + b$$

$$Y = XY^2 + a \quad .$$

The Y-equation in form (3) is $Y = [a] + [XY]\ Y$ and so we have that $Y \supseteq (Xa)^*a$. Substituting this in the X-equation, we get $X \supseteq X^3(Xa)^*a^2 + X(Xa)^*a^3 + b$, or in the form of (3),

$$X \supseteq [b] + [X^2(Xa)^*a^2 + (Xa)^*a^3]X$$

whose solution is

$$X \supseteq \{(ba)^*b^2a^2 + (ba)^*a^3\}^*b,$$

whence from $Y \supseteq (Xa)^*a$ we get

$$Y \supseteq \{\{(ba)^*b^2\,a^2 + (ba)^*a^3\}^*ba\}^*a.$$

As a final remark, it seems that Parikh's theorem is most naturally stated in terms of regular commutative events, but since he uses instead the notion of semi-linear events, we briefly explain the relationship.

Definition. A subset E of N^n is said to be *linear* if there exist members

$$\alpha, \beta_1, \ldots, \beta_m \text{ of } N^n$$

such that

$$E = \{w \mid w = \alpha + n_1\,\beta_1 + \ldots + n_m\,\beta_m,\ n_i \in N\}.$$

E is said to be *semi-linear* if E if the union of a finite number of linear sets.

A word $A^a B^b C^c \ldots$, where $\{A, B, C, \ldots\}$ is a commutative alphabet, then corresponds to the vector $(a, b, c, \ldots)$ and a semi-linear event in Parikh's sense corresponds to a finite sum of events of the form $w_1{}^* w_2{}^* \ldots w_k{}^* w_0$ where the w_i are words in $A, B, C, \ldots$ But the sum and product of two events in this form can be expressed in this form using the associative, distributive and commutative laws, and the star of an event in this form can be put into this form using also the laws $(E+F+G+\ldots)^* = E^*F^*G^*\ldots$ and $(E^*F^*)^* = 1+E^*F^*F$. So every regular event over a commutative alphabet can be put in semi-linear form. As an example, we display the solutions obtained above in this form:

$$X = b+(ba)^*(a^3)^*a^2 b^3+(ba)^*(a^3)^*a^3 b$$
$$Y = a+(ba)^*(a^3)^*a^4 b^3+(ba)^*(a^3)^*a^5 b+(ba)^*a^2 b.$$

Acknowledgment

The author is grateful to Dr. J. H. Conway for many helpful conversations in the writing of this paper.

References

1. R. J. Parikh, " On context-free languages ", *J. Assoc. Comput. Mach.* (13), 4 (1966), 570–581.
2. J. H. Conway, *Regular algebras and finite automata* (Chapman-Hall, 1971).

32–03,211 Street,
Bayside, New York, U.S.A.