Factor Theory Revisited

Roland Backhouse

February 2001

Introduction

"Factors" and the "factor matrix" were introduced by Conway (1971).

He used them very effectively in, for example, constructing biregulators.

Conway's discussion is wordy, making it difficult to understand. There are also occasional errors which are difficult to detect and add to the confusion. ("The theorem does prevent E from occurring twice" should read "The theorem does *not* prevent E from occurring twice.")

We show how to reproduce Conway's results by formal calculation.

Also show how factors and "co-reflexive" factors (weakest liberal preconditions) are used in a calculational, point-free proof of Newman's lemma.

Factors

$$L{\cdot}M \subseteq N \quad \equiv \quad M \subseteq L\backslash N$$

$$L{\cdot}M \subseteq N \quad \equiv \quad L \subseteq N/M$$

(Also called “residuals” and “weakest prespecifications”.)

Matrices

No need to restrict discussion to regular languages.

Factor "matrix" exists for arbitrary languages.

Factor "matrix" of language E has finite dimension equivales E is regular.

Let $\mathcal{I}$ be any set (the *index* set). A (square) *matrix* of dimension $\mathcal{I}$ is a function with domain $\mathcal{I}\times\mathcal{I}$.

The matrices we consider will have range the carrier set of a regular algebra. Sum, product etc. are extended to matrices in the usual way.

Suppose $\mathbf{M} \in \mathcal{A}\leftarrow\mathcal{I}\times\mathcal{I}$ is a matrix. If i and j are elements of $\mathcal{I}$ then the application of $\mathbf{M}$ to (i,j) is denoted $\mathsf{i}\,\mathbf{M}\,\mathsf{j}$ and is called *the* (i,j)th *element of* $\mathbf{M}$. Unit matrix is denoted by $\mathbf{I}$.

Left and Right Factors

Let E denote a fixed element of $\mathcal{A}$.

A *factor* of E is any element of $\mathcal{A}$ that can be expressed in the form $\mathsf{X}\backslash\mathsf{E}/\mathsf{Y}$ for some X and Y.

An element of $\mathcal{A}$ is a *left factor* of E if it can be expressed in the form E/Y for some Y and a *right factor* of E if it can be expressed in the form $\mathsf{X}\backslash\mathsf{E}$ for some X.

Let $\mathcal{I}$ be some index set and suppose X_i is a language for each $i{\in}\mathcal{I}$. Then the function

$$\langle i,j{::}\ \mathsf{X}_i\backslash\mathsf{E}/\mathsf{X}_j\rangle$$

is a matrix of factors of E.

Need to identify the index set.

Reflexivity and Transitivity

For any indexed set of languages X_i $(i \in \mathcal{I})$ the matrix $\langle i,j{::}\,X_i\backslash X_j\rangle$ is reflexive and transitive.

Reflexivity follows from

$$I \subseteq L\backslash L \quad .$$

Transitivity follows from

$$\begin{array}{ll}
 & L\backslash M \cdot M\backslash N \subseteq L\backslash N \\
\equiv & \{ \quad \text{Galois connection defining factors} \quad \} \\
 & L \cdot L\backslash M \cdot M\backslash N \subseteq N \\
\Leftarrow & \{ \quad \text{cancellation: } L \cdot L\backslash M \subseteq M \\
 & \quad\;\; \text{monotonicity of product and transitivity of } \subseteq \quad \} \\
 & M \cdot M\backslash N \subseteq N \\
\equiv & \{ \quad \text{cancellation} \quad \} \\
 & \mathsf{true} \quad .
\end{array}$$

One-one correspondence

Define the functions $\triangleleft$ and $\triangleright$ by

$$\begin{aligned} X\triangleleft &= E/X \quad , \\ X\triangleright &= X\backslash E \quad . \end{aligned}$$

By definition, the range of $\triangleleft$ is the set of *left* factors of E and the range of $\triangleright$ is the set of *right* factors of E.

We also have the Galois connection:

$$X \subseteq Y\triangleleft \;\equiv\; Y \subseteq X\triangleright \quad .$$

Hence,

$$\begin{aligned} X\triangleleft\triangleright\triangleleft &= X\triangleleft \quad , \\ X\triangleright\triangleleft\triangleright &= X\triangleright \quad , \\ E\triangleleft\triangleright = E &= E\triangleright\triangleleft \quad . \end{aligned}$$

The Factor Matrix

Let $\mathcal{L}$ denote the set of left factors of E.

Define the *factor matrix* of E to be the binary operator $\backslash$ restricted to $\mathcal{L}\times\mathcal{L}$. Thus entries in the matrix take the form $\mathsf{L}_0\backslash\mathsf{L}_1$ where L_0 and L_1 are left factors of E.

This is a reflexive, transitive matrix.

Also, by definition of a left factor and a factor, all entries in the matrix are factors of E.

The row and column containing the left and right factors, respectively, is given by:

$$\begin{aligned}
\mathsf{U}\backslash\mathsf{E}/\mathsf{V} &= \mathsf{U}\!\rhd\!\lhd\backslash\mathsf{V}\!\lhd \ , \\
\mathsf{V}\!\lhd &= \mathsf{E}\!\lhd\backslash\mathsf{V}\!\lhd \ , \\
\mathsf{U}\!\rhd &= \mathsf{U}\!\rhd\!\lhd\backslash\mathsf{E}\!\rhd\!\lhd \ , \\
\mathsf{E} &= \mathsf{E}\!\lhd\backslash\mathsf{E}\!\rhd\!\lhd \ .
\end{aligned}$$

Factors

$$L{\cdot}M \subseteq N \quad\equiv\quad M \subseteq L\backslash N$$

$$L{\cdot}M \subseteq N \quad\equiv\quad L \subseteq N/M$$

Coreflexive Factors

(Weakest liberal preconditions. Möller's $S{\rightarrow}B$ and $B{\leftarrow}S$.)

For all relations S and coreflexive relations B , $S \underline{\backslash} B$ and $B \underline{/} S$ are coreflexive relations such that, for all coreflexive relations A:

$$A \;\subseteq\; S \underline{\backslash} B \quad\equiv\quad (S{\circ}A){<} \;\subseteq\; B \quad .$$

$$A \;\subseteq\; B \underline{/} S \quad\equiv\quad (A{\circ}S){>} \;\subseteq\; B \quad .$$

(A relation A is coreflexive if $A \;\subseteq\; I$ where I denotes the identity relation.)

Newman's Lemma

(Doornbos, Backhouse and Van der Woude, TCS 1997)

Any relation that admits induction and is "locally confluent" is also "confluent".

Relation R is *confluent* is equivalent to

$$R^* \circ (R^\cup)^* \;\subseteq\; (R^\cup)^* \circ R^* \quad .$$

Relation R is *locally confluent* if

$$R \circ R^\cup \;\subseteq\; (R^\cup)^* \circ R^* \quad .$$

Because it turns out that it is not essential for the proof of the lemma that the relations are each other's converse, we generalise to

$$R^* \circ S^* \;\subseteq\; S^* \circ R^*$$

follows if $R \cup S^\cup$ admits induction and

$$R \circ S \;\subseteq\; S^* \circ R^* \quad .$$

Admits Induction

The assumption that $R \cup S^{\cup}$ admits induction is equivalent to, for all coreflexives A:

$$R \underline{\backslash} A \circ A \underline{/} S \ \subseteq \ A \quad \Rightarrow \quad I \subseteq A \quad .$$

The goal is to calculate a condition on R and S guaranteeing that

$$R^* \circ S^* \ \subseteq \ S^* \circ R^* \quad .$$

In order to use that $R \cup S^{\cup}$ admits induction one has to invent an "induction hypothesis" —a coreflexive A such that

$$I \subseteq A \ \equiv \ R^* \circ S^* \subseteq S^* \circ R^* \quad .$$

Calculating the Induction Hypothesis

$$
\begin{array}{ll}
 & R^* \circ S^* \subseteq S^* \circ R^* \\
\equiv & \{ \quad I \text{ is the identity of composition} \quad \} \\
 & R^* \circ I \circ S^* \subseteq S^* \circ R^* \\
\equiv & \{ \quad \text{factors} \quad \} \\
 & I \subseteq R^* \backslash (S^* \circ R^*) / S^* \\
\equiv & \{ \quad I \subseteq I, \text{ infima} \quad \} \\
 & I \subseteq R^* \backslash (S^* \circ R^*) / S^* \cap I \quad .
\end{array}
$$

Completing the Proof

Introduce the shorthand A for $R^*\backslash(S^*\circ R^*)/S^* \cap I$. Then, for all coreflexives B:

$$B \subseteq A \quad \equiv \quad R^* \circ B \circ S^* \subseteq S^* \circ R^* \quad .$$

By instantiating B to A we obtain the *cancellation* property:

$$R^* \circ A \circ S^* \subseteq S^* \circ R^* \quad .$$

Completing the Proof (Continued)

$$
\begin{array}{ll}
 & I \subseteq R^*\backslash(S^*\circ R^*)/S^* \cap I \\
\equiv & \{ \quad \text{definition of } A \quad \} \\
 & I \subseteq A \\
\Leftarrow & \{ \quad \bullet \quad R \cup S^{\cup} \text{ admits induction} \quad \} \\
 & R\mathbin{\underline{\backslash}}A \circ A\mathbin{\underline{/}}S \subseteq A \\
\equiv & \{ \quad \text{characterisation of } A\text{: for all coreflexives } B, \\
 & \qquad B \subseteq A \;\equiv\; R^* \circ B \circ S^* \subseteq S^* \circ R^*, \\
 & \qquad B := R\mathbin{\underline{\backslash}}A \circ A\mathbin{\underline{/}}S \quad \} \\
 & R^* \circ R\mathbin{\underline{\backslash}}A \circ A\mathbin{\underline{/}}S \circ S^* \;\subseteq\; S^* \circ R^* \\
\equiv & \{ \quad \text{regular algebra: } X^* = I \cup X\circ X^* = I \cup X^*\circ X \quad \} \\
 & \quad R^* \circ R\mathbin{\underline{\backslash}}A \circ A\mathbin{\underline{/}}S \;\subseteq\; S^* \circ R^* \\
 & \wedge\; R\mathbin{\underline{\backslash}}A \circ A\mathbin{\underline{/}}S \circ S^* \;\subseteq\; S^* \circ R^* \\
 & \wedge\; R^* \circ R \circ R\mathbin{\underline{\backslash}}A \circ A\mathbin{\underline{/}}S \circ S \circ S^* \;\subseteq\; S^* \circ R^* \quad .
\end{array}
$$

Completing the Proof (1st, 2nd conjuncts)

$$
\begin{array}{lll}
 & R^* \circ R\backslash A \circ A/S & \\
\subseteq & \{ \quad I \text{ is unit of composition;} \quad R\backslash A \circ A/S \subseteq I \circ I \subseteq I \quad \} & \\
 & I \circ R^* \circ I & \\
\subseteq & \{ \quad S^* \text{ is reflexive:} \quad I \subseteq S^* \quad \} & \\
 & S^* \circ R^* \quad . &
\end{array}
$$

Similarly for the 2nd conjunct.

Completing the Proof (3rd Conjunct)

$$
\begin{array}{ll}
 & R^* \circ R \circ R\backslash A \circ A/S \circ S \circ S^* \\
\subseteq & \{ \quad R \circ R\backslash A \subseteq A \circ R, \quad A/S \circ S \subseteq S \circ A \quad \} \\
 & R^* \circ A \circ R \circ S \circ A \circ S^* \\
\subseteq & \{ \quad \bullet \quad \text{local confluence:} \quad R \circ S \subseteq S^* \circ R^* \quad \} \\
 & R^* \circ A \circ S^* \circ R^* \circ A \circ S^* \\
\subseteq & \{ \quad \text{cancellation property:} \quad R^* \circ A \circ S^* \subseteq S^* \circ R^* \quad \} \\
 & S^* \circ R^* \circ R^* \circ A \circ S^* \\
= & \{ \quad R^* \text{ is transitive} \quad \} \\
 & S^* \circ R^* \circ A \circ S^* \\
\subseteq & \{ \quad \text{cancellation property:} \quad R^* \circ A \circ S^* \subseteq S^* \circ R^* \quad \} \\
 & S^* \circ S^* \circ R^* \\
= & \{ \quad S^* \text{ is transitive} \quad \} \\
 & S^* \circ R^* \quad .
\end{array}
$$