Notes on Petri Nets and Attack Trees

Aubrey Bryant and Harley Eades III

July 30, 2018

Abstract

TODO

$$\begin{tikzcd}
 & A & \\
B \arrow[ur, "f" description] \arrow[r, "i"] & C \arrow[u, "g" description] & D \arrow[ul, "h" description] \arrow[l, "j"']
\end{tikzcd}$$

1 Notes on Attack Trees and Petri Nets

Definition 1. *A **finite multiset** over a set S can be defined as a formal sum: $n_1a_1, \oplus ... \oplus, n_ia_i$.*

- $n_1, ...n_i \in \mathbb{N}$, *and* $a_1, ...a_i \in S$,
- *na: a occurs n times in multiset,*
- $na_i \oplus ma_j = ma_j \oplus na_i$,
- $na \oplus ma = (m + n)a$,
- $na \oplus 0 = na = 0 \oplus na$.

Definition 2. *The **free commutative monoid** generated by the set A is the set of all finite multisets drawn from A, where:*

- *The monoidal operation is the formal sum of multisets,*
- *The monoidal unit is $\emptyset$.*

Definition 3. *A **graph**, (V, T, src, tar), consists of the following structure:*

- *A set of nodes V,*
- *A set of edges T,*
- *A source function src: $T \longrightarrow V$,*
- *A target function tar: $V \longrightarrow T$.*

Definition 4. *A **graph morphism**, $h : G \longrightarrow G'$, between graphs is a pair (f, g) where:*

- *f: $T \longrightarrow T'$ is a function,*
- *g: $V \longrightarrow V'$ is a function.*

Definition 5. *Original defn: A **Petri net**, (P, T, F, M_0), consists of the following structure:*

- *A finite set of places P,*
- *A finite set of transitions T that is disjoint from P,*
- *A causal dependency relation F: $(P \times T) + (T \times P) \longrightarrow \mathbb{N}^+$,*
- *An initial marking M_0.*

Definition 6. *A **Petri net**, (S, T, src, tar), is a graph consisting of:*

- *A finite set of places S for nodes,*
- *A finite set of transitions T for arcs,*
- *Functions $src, tar : T \longrightarrow S^{\oplus}$.*

Definition 7. *A **monoid homomorphism** between two monoids $(M_1, \oplus_1, 0_1)$ and $(M_2, \oplus_2, 0_2)$ is a function $f : M_1 \longrightarrow M_2$ such that:*

- $f(a_1 \oplus_1 a_2) = f(a_1) \oplus f(a_2)$
- $f(0_1) = 0_2$

Definition 8. *A **Petri net morphism** between two Petri nets $(T_1, S_1^{\oplus})$ and $(T_2, S_2^{\oplus})$ is a graph morphism (f, g) where $g : S_1^{\oplus} \longrightarrow S_2^{\oplus}$ is a monoid homomorphism.*

Thus, take as objects Petri nets $(T, S^{\oplus})$ and as morphisms Petri net morphisms. This defines a category Petri.

Lemma 9. *Suppose we have two Petri nets, $(S_1, \oplus, 0)$ and $(S_2, \oplus, 0)$.*

$$(S_1^{\oplus} \times S_2^{\oplus}) \cong (S_1 + S_2)^{\oplus}$$

Proof. To show this, we need to define two homomorphisms between them, which we will call F and G.

It is important to note that the $\oplus$ operation is commutative. This commutativity allows the elements of the resulting free commutative monoid (FCM) to be rearranged, which will help us in our proof by allowing FCMs to be sorted in the following way:

Consider an arbitrary $s \in (S_1 + S_2)^{\oplus}$. Since the generator is the disjoint union of S_1 and S_2, the elements of s are drawn from those two sets, but are not grouped according to their origin set. Using commutativity, we can move all $y_i \in S_1$ to the front, and all $z_j \in S_2$ to the end. Then the form of s is $(\oplus_i y_i) \oplus (\oplus_j z_j)$, where the elements are grouped according to their origin set. Any element of $(S_1 + S_2)^{\oplus}$ can be similarly sorted. For the purposes of this proof, assume that all such elements are so sorted.

Now, let us define the function F: $(S_1 + S_2)^{\oplus} \longrightarrow (S_1^{\oplus} \times S_2^{\oplus})$.
Let k be an arbitrary element of $(S_1 + S_2)^{\oplus}$. We know that $k \in (S_1 + S_2)^{\oplus}$ must have the form $(\oplus_i y_i) \oplus (\oplus_j z_j)$, where $y_i \in S_1$ and $z_i \in S_2$ as described above. Furthermore, since the + operator is disjoint union, each element includes a marker indicating its origin

set, which we can use to locate the boundary between elements of S_1 and elements of S_2. Therefore we can define F as follows:

$$F((\oplus_i y_i \in S_1) \oplus (\oplus_j z_j \in S_2)) = ((\oplus_i y_i \in S_1), (\oplus_j z_j \in S_2))$$

$$F((S_1, \oplus) \oplus (S_2, \oplus)) = ((S_1, \oplus), (S_2, \oplus))$$

This allows an element of $(S_1 + S_2)^{\oplus}$ to be matched with an element of $(S_1^{\oplus} \times S_2^{\oplus})$, since the generator of $(S_1 + S_2)^{\oplus}$ contains the generator for both $S_1^{\oplus}$ and $S_2^{\oplus}$.

Another important feature of FCMs arises from lifting the coproducts of sets to FCMs. For the coproduct of sets, we know that there exist the following functions:

$$inj_1 : S_1 \longrightarrow (S_1 + S_2)$$

$$inj_2 : S_2 \longrightarrow (S_1 + S_2)$$

Likewise, for the coproduct of FCMs, there are the functions:

$$inj_1^{\oplus} : S_1^{\oplus} \longrightarrow (S_1 + S_2)^{\oplus}$$

$$inj_1^{\oplus}(\oplus_i n_i x_i) = \oplus_i n_i (inj_1 x_i)$$

$$inj_2^{\oplus} : S_2^{\oplus} \longrightarrow (S_1 + S_2)^{\oplus}$$

$$inj_2^{\oplus}(\oplus_i n_i x_i) = \oplus_i n_i (inj_2 x_i)$$

Using this property, let us now define $G : (S_1^{\oplus} \times S_2^{\oplus}) \longrightarrow (S_1 + S_2)^{\oplus}$.
Let k be an arbitrary element of $(S_1^{\oplus} \times S_2^{\oplus})$. We know k must have the form (M_1, M_2) where M_i is a multiset of the form $(n_1 z_1 \oplus ... \oplus n_b z_b)$, and all $z \in S_i$ for $i \in \{1, 2\}$ (all n being natural number counters for the multiset).
Therefore we define the function G as follows:

$$G(M_1, M_2) = (inj_1^{\oplus} M_1) \oplus (inj_2^{\oplus} M_2)$$

By this transformation, we can match an element of $(S_1^{\oplus} \times S_2^{\oplus})$ with an element of $(S_1 + S_2)^{\oplus}$, since by the nature of coproducts, any s $\in S_1^{\oplus} \in (S_1 + S_2)^{\oplus}$, and similarly any s $\in S_2^{\oplus} \in (S_1 + S_2)^{\oplus}$.

Now that we have defined a homomorphism in both directions, we must prove that $F; G = Id$ and $G; F = Id$. Take an arbitrary multiset M of the form $(n_1 z_1 \oplus ... \oplus n_b z_b)$, with some elements drawn from a set S_a and some drawn from S_b and each $n_i \in \mathbb{N}$. Sorting this multiset will yield the form $(\oplus_a n_a y_a) \oplus (\oplus_b n_b z_b)$, where $y_a \in S_a$ and $z_b \in S_b$. Putting this into the functions, we get:

$$\begin{aligned} G(F((\oplus_a n_a y_a) \oplus (\oplus_b n_b z_b))) &= G((\oplus_a n_a y_a), (\oplus_b n_b z_b)) \\ &= (\oplus_a n_a y_a) \oplus (\oplus_b n_b z_b) \end{aligned}$$

Thus, $F; G = Id$.

Now let us check for identity in the opposite direction, proving G;F = Id. Take arbitrary sets S_a and S_b. Generate the FCM of each and then their product: $(S_a^{\oplus} \times S_b^{\oplus})$. The result will have the form $((\oplus_a n_a y_a), (\oplus_b n_b z_b))$, where $y_a \in S_a$ and $z_b \in S_b$. Putting this into the functions, we get:

$$G((\oplus_a n_a y_a), (\oplus_b n_b z_b)) = ((\oplus_a n_a y_a) \oplus (\oplus_b n_b z_b))$$

$$F((\oplus_a n_a y_a) \oplus (\oplus_b n_b z_b)) = ((\oplus_a n_a y_a), (\oplus_b n_b z_b))$$

Thus, G;F = Id. Since $(S_1^{\oplus} \times S_2^{\oplus}) \leftrightarrow (S_1 + S_2)^{\oplus}$, we can conclude that $(S_1^{\oplus} \times S_2^{\oplus}) \cong (S_1 + S_2)^{\oplus}$.

□

Definition 10. *A **chainable petri net**, (S, T, src, tar, i, f) is a Petri net with the following additional features:*

- *An element i that is the starting point for the net. If the initial marking is $(s_1 \oplus s_2 ... \oplus s_n)$, then $i \longrightarrow (s_1 \oplus s_2 ... \oplus s_n)$, with elements not duplicated: $s_j \neq s_k$ when $j \neq k$. Also, $\emptyset \longrightarrow i$. That is, i cannot be reached from within the net.*
- *An element f that is the endpoint of the net. If the final marking is $(s_1 \oplus s_2 ... \oplus s_n)$, $(s_1 \oplus s_2 ... \oplus s_n) \longrightarrow f$, and $f \longrightarrow \emptyset$.*
- *Morphisms for chainable nets must preserve both i and f. So, a morphism $< a, b >$: $(N, i, f) \longrightarrow (N', i', f')$ is an ordinary net morphism that preserves the markings $b(i) = i'$ and $b(f) = f'$.*

The chainable petri net, or CNET, is a petri net that tracks both its initial and its final places, to facilitate chaining the petri net together with other petri nets at either end. This enables the use of operators such as SEQ, AND, & OR.
Suppose we have two CNETs, (N_1, i_1, f_1) and (N_2, i_2, f_2).
$N_1 = (src, tar : T \longrightarrow S^{\oplus})$ and $N_2 = (src', tar' : T' \longrightarrow S'^{\oplus})$.

SEQ for CNETs is the composition operation:
$N_1 \; ; N_2 = T + T' \longrightarrow S^{\oplus} + S'^{\oplus}$;
$i = i_1$;
$f = f_2$;
$f_1 \longrightarrow i_2$;
$i_2 \longrightarrow f_1$.

OR for CNETs is the coproduct(p.126):
$N_1 + N_2 = (T_1 + T_2) \longrightarrow ((S_1 + S_2)^{\oplus} + i_3 + f_3)$;
$i_3 = i_1 \oplus i_2$; f_3 is a new place with the following new transitions:
$f_1 \longrightarrow f_3$;
$f_2 \longrightarrow f_3$;
$f_3 \longrightarrow \emptyset$.

Example 11. *Now we will examine disjunction (OR) in CNETs, starting with a basic example. Consider an ordinary Petri net (P_x, T_x, src_x, tar_x). A simple model of the disjunction $p_3 OR p_4$ is given by the following relations:*

- *Let $P = \{p_1, p_2, p_3\}$, and src_x, tar_x: $(p_1) \longrightarrow (p_3)$, and $(p_2) \longrightarrow (p_3)$.*
- *Given this relation, as long as p_1, p_2, or both are activated, p_3 will be activated.*
- *If neither p_1 nor p_2 are activated, p_3 will also remain inactive.*

Within a single Petri net, we can see that disjunction is modeled graphically by two transition arcs leading to one place. If either transition fires, the place will be activated, enabling its subsequent transition(s) to fire. The disjunction of two CNETs will result in a similar pattern: if at least one of the CNET disjuncts reaches its final marking, then the disjunction itself will reach its final marking.

Definition 12. *Given two CNETs, $N_1 = (P_1, T_1, src_1, tar_1, i_1, f_1)$ and $N_2 = (P_2, T_2, src_2, tar_2, i_2, f_2)$, their* ***disjunction*** *is $N_1 \oplus N_2$, where: * NOTE WHY IS IT $\oplus$ and not $+$?*

- *$T = T_1 + T_2$,*
- *$P = ((P_1 + P_2) + (i_1, i_2) + f_1 + f_2)$ (note: if the initial places are paired why does this not result in AND behavior? The choice part happens in the final places? Did not pair the final places to make it possible to finish one and not the other, and still complete the firing.)*
- *$[src_1, src_2], [tar_1, tar_2] : T \longrightarrow P^{\oplus}$. (indicating we should use the appropriate function depending on origin set)*
- *The initial place $i = i_1 \oplus i_2$;*
- *The final place f.*

Lemma 13. *The disjunction of two CNETs, $N_1 + N_2$, is the coproduct.*

Proof. $N_1 + N_2$ is a coproduct if it satisfies the following conditions: it must have morphisms $i_1 : N_1 \longrightarrow N_1 + N_2$ and $i_2 : N_2 \longrightarrow N_1 + N_2$ such that for any object R and morphisms $f_1 : N_1 \longrightarrow R$ and $f_2 : N_2 \longrightarrow R$, there is a unique morphism $[f_1, f_2] : N_1 + N_2 \longrightarrow R$ such that $f_1 = i_1; [f_1, f_2]$ and $f_2 = i_2; [f_1, f_2]$.

Let $A = (S_A, T_A, i_A, f_A)$ and $B = (S_B, T_B, i_B, f_B)$, and take A + B. We have $i_A : A \longrightarrow A + B$ and $i_B : B \longrightarrow A + B$ by lifting the coproduct of sets to the coproduct of CNETs. Specifically, $S_{A+B} = (S_A + S_B + i_{A+B} + f_{A+B})$, and $T_{A+B} = (T_A + T_B + (i_{A+B}, i_A \oplus i_B) + (f_A, f_{A+B}) + (f_B, f_{A+B}) + (f_A \oplus f_B, f_{A+B}))$. Since these are all coproducts, we can rely on their injections to yield the injections of the larger structure.

Given another CNET C and morphisms $f_1 : A \longrightarrow C$ and $f_2 : B \longrightarrow C$, we define $[f_1, f_2]$ as follows:

$$f(x) = \begin{cases} f_1(x), & \text{if x is from A} \\ f_2(x), & \text{if x is from B} \end{cases} \tag{1}$$

Given this definition of $[f_1, f_2]$, it is clear that $f_1 = inj_1; [f_1, f_2]$ and $f_2 = inj_2; [f_1, f_2]$. To show that this satisfies the uniqueness requirement, let us consider an arbitrary function $h : (A + B) \longrightarrow C$, where $h; inj_A = f_1$ and $h; inj_B = f_2$. For $a \in A$ and $b \in B$, the following equalities hold:

$$h(a) = inj_A(a); h(a) = h_A(a); inj_A(a) = f_1(a) = [f_1, f_2](a) \tag{2}$$

$$h(b) = inj_B(b); h(b) = h_B(b); inj_B(b) = f_2(b) = [f_1, f_2](b) \tag{3}$$

Thus, $h = [f_1, f_2]$, showing that f is unique. This provides a morphism as required, showing that the CNET disjunction is a coproduct.

□

Example nets: K =
$S_K : \{a, b, c\}$
$T_K : \{t\}$
$F_K(a, t) = 2$
$F_K(b, t) = 1$
$F_K(t, c) = 2$
$F_K(else) = 0$
$S_K^{\oplus} : \{2a \oplus 1b \oplus 2c\}$
$t = \{2a \oplus 1b \longrightarrow 2c\}$
$\delta_{0K}(t) = 2a \oplus 1b\}$
$\delta_{1K}(t) = 2c\}$
M =
$S_M : \{d, e\}$
$T_M : \{t'\}$
$F_M(d, t') = 2$
$F_M(t', e) = 1$
$F_M(else) = 0$
$S_M^{\oplus} : \{2d \oplus 1e\}$
$t = \{2d \longrightarrow 1e\}$
$\delta_{0M}(t') = 2d\}$
$\delta_{1M}(t') = 1e\}$
$S_K^{\oplus} \times S_M^{\oplus} = (2a \oplus 1b, 2d) \longrightarrow (2c, 1e)$
$(S_K + S_M)^{\oplus} = (\{1\} \times S_K) \cup (\{2\} \times S_M)^{\oplus}$
$((1, 2a), (1, 1b), (2, 2d))^{\oplus} =$
$S_{KM}^{\oplus} : \{(1, 2a), (1, 1b), (2, 2d)\}$
$T_{KM} : \{t_1, t_2\}$
$t_1 = ((1, 2a) \oplus (1, 1b)) \longrightarrow (1, 2c)$
$t_2 = (2, 2d) \longrightarrow (2, 1e)$
$\delta_{0KM}(t_1) = (1, 2a) \oplus (1, 1b)\}$
$\delta_{0KM}(t_2) = (2, 2d)\}$
$\delta_{1KM}(t_1) = (1, 2c)\}$
$\delta_{1KM}(t_2) = (2, 1e)\}$
$(S_1^{\oplus} \times S_2^{\oplus})$ and $(S_1 + S_2)^{\oplus}$ are isomorphic.

Suppose there are two Petri nets $S_1 andS_2$, with sets of places $M_1 andM_2$ and sets of arcs $T_1 andT_2$.
Let F be the homomorphism from $(S_1 + S_2)^{\oplus}$ to $(S_1^{\oplus} \times S_2^{\oplus})$.
$F((S_1 + S_2)^{\oplus}) = (S_1^{\oplus} + S_2^{\oplus})$
where $S_1 + S_2 = (\{1\} \times S_1) \cup (\{2\} \times S_2)$
For F:
Calculating the set of places of the codomain:
$S_1 = \bigcup_{y \in domain(x,y)} |x = 1)$
$S_2 = \bigcup_{y \in domain(x,y)} |x = 2)$
Note: I mean to separate out the two sets using the disjoint markers here.
The set of places of the codomain = $(S_1^{\oplus} \times S_2^{\oplus})$
The arrows of the codomain maintain the structure defined in the domain, disregarding

the origin markers $\{1\}$ and $\{2\}$ added in by taking the disjoint union.
Since the function preserves the structure between the objects, only changing the names of the objects, this is a homomorphism.
Now, let G be the homomorphism from $(S_1^{\oplus} \times S_2^{\oplus})$ to $(S_1 + S_2)^{\oplus}$.
The objects or places of the codomain are the objects of the domain modified in the following way:
where objects in the domain have the form $(x, y), (\{1\} \times x) \cup (\{2\} \times y)$.
The arrows of the codomain maintain the structure of the domain, adding in origin markers $\{1\}$ and $\{2\}$ by position as described above.
Since G preserves the group's structure and only modifies objects' names, it is a homomorphism. Clearly,$G \circ F = F \circ G$, since F removes the origin markings $\{1\}$ and $\{2\}$ and G puts them back. Structure remains unchanged in either direction.

References