Booleovské funkce - druhá část

Definice. Ať je G konečná komutativní grupa a R okruh. Pro zobrazení $h, \tilde{h} : G \to R$ definujeme *(diskrétní) konvoluci* $h \otimes \tilde{h} : G \to R$ takto:

$$(h \otimes \tilde{h})(a) = \sum_{b \in G} h(b) \cdot \tilde{h}(a - b)$$

Obraz v konvoluci můžeme také zapsat jako

$$(h \otimes \tilde{h})(a) = \sum_{\substack{(b,c) \in G \times G \\ b+c=a}} h(b) \cdot \tilde{h}(c)$$

Pro zobrazení $(h \otimes \tilde{h}) \otimes \bar{h}$ pak dostaneme:

$$\begin{aligned}
((h \otimes \tilde{h}) \otimes \bar{h})(a) &= \sum_{\substack{(d',d) \in G \times G \\ d'+d=a}} (h \otimes \tilde{h})(d') \cdot \bar{h}(d) \\
&= \sum_{\substack{(d',d) \in G \times G \\ d'+d=a}} \left(\sum_{\substack{(b,c) \in G \times G \\ b+c=d'}} h(b) \cdot \tilde{h}(c) \right) \cdot \bar{h}(d) \\
&= \sum_{\substack{(d',d) \in G \times G \\ d'+d=a}} \sum_{\substack{(b,c) \in G \times G \\ b+c=d'}} h(b) \cdot \tilde{h}(c) \cdot \bar{h}(d) \\
&= \sum_{\substack{(b,c,d) \in G \times G \times G \\ b+c+d=a}} h(b) \cdot \tilde{h}(c) \cdot \bar{h}(d)
\end{aligned}$$

Konvoluce je tedy asociativní binární operace na množině všech zobrazení $G \to R$. Je-li navíc R komutativní okruh, konvoluce je také komutativní.

Lemma. Pro $f, g \in \mathrm{R}_n$ platí

$$\mathrm{W}(\widehat{f+g}) = \mathrm{W}(\widehat{f}\,) \otimes \mathrm{W}(\widehat{g}\,)$$

Tedy spektrum součtu binárních booleovských funkcí je konvoluce jejich spekter.

Důkaz. Vyjádříme hodnotu $\widehat{f+g}$ v $z \in \mathbb{F}_2^n$:

$$\begin{aligned}
\widehat{f+g}\,(z) &= \widehat{f}(z) \cdot \widehat{g}(z) \\
&= \left(\sum_{v \in \mathbb{F}_2^n} \mathrm{W}(\widehat{f}\,)(v) \cdot \widehat{\mathrm{p}}_v \right)(z) \cdot \left(\sum_{w \in \mathbb{F}_2^n} \mathrm{W}(\widehat{g}\,)(w) \cdot \widehat{\mathrm{p}}_w \right)(z)
\end{aligned}$$

$$= \left(\sum_{v\in\mathbb{F}_2^n} \mathrm{W}(\widehat{f})(v)\cdot\widehat{\mathrm{p}}_v(z)\right)\cdot\left(\sum_{w\in\mathbb{F}_2^n} \mathrm{W}(\widehat{g})(w)\cdot\widehat{\mathrm{p}}_w(z)\right)$$

$$= \sum_{v\in\mathbb{F}_2^n}\sum_{w\in\mathbb{F}_2^n} \mathrm{W}(\widehat{f})(v)\cdot\mathrm{W}(\widehat{g})(w)\cdot\widehat{\mathrm{p}}_{v+w}(z)$$

$$\overset{(u=v+w)}{=} \sum_{v\in\mathbb{F}_2^n}\sum_{u\in\mathbb{F}_2^n} \mathrm{W}(\widehat{f})(v)\cdot\mathrm{W}(\widehat{g})(u+v)\cdot\widehat{\mathrm{p}}_u(z)$$

$$= \sum_{u\in\mathbb{F}_2^n}\left(\sum_{v\in\mathbb{F}_2^n} \mathrm{W}(\widehat{f})(v)\cdot\mathrm{W}(\widehat{g})(u+v)\right)\cdot\widehat{\mathrm{p}}_u(z)$$

$$= \sum_{u\in\mathbb{F}_2^n}\left(\mathrm{W}(\widehat{f})\otimes\mathrm{W}(\widehat{g})\right)(u)\cdot\widehat{\mathrm{p}}_u(z)$$

$$= \left(\sum_{u\in\mathbb{F}_2^n}\left(\mathrm{W}(\widehat{f})\otimes\mathrm{W}(\widehat{g})\right)(u)\cdot\widehat{\mathrm{p}}_u\right)(z)$$

Máme tedy

$$\widehat{f+g} = \sum_{u\in\mathbb{F}_2^n}\left(\mathrm{W}(\widehat{f})\otimes\mathrm{W}(\widehat{g})\right)(u)\cdot\widehat{\mathrm{p}}_u$$

Pro každé $u\in\mathbb{F}_2^n$ musí platit $\mathrm{W}(\widehat{f+g})(u) = \left(\mathrm{W}(\widehat{f})\otimes\mathrm{W}(\widehat{g})\right)(u)$. □

Například $\widehat{1}_{\mathrm{R}_n} = \widehat{\mathrm{const}_1} = -\widehat{\mathrm{const}_0} = -\widehat{\mathrm{p}}_0$ je zápis funkce $\widehat{1}_{\mathrm{R}_n}$ v bázi znaménkových funkcí parit. Snadno zjistíme, že pro $f\in\mathrm{R}_n$ je $\mathrm{W}(\widehat{f+1_{\mathrm{R}_n}}) = -\mathrm{W}(\widehat{f})$.
Pro $f\in\mathrm{R}_n$ a $u,v\in\mathbb{F}_2^n$ platí:

$$\mathrm{W}(\widehat{f+\mathrm{p}_v})(u) = \left(\mathrm{W}(\widehat{f})\otimes\mathrm{W}(\widehat{\mathrm{p}}_v)\right)(u) = \sum_{w\in\mathbb{F}_2^n}\mathrm{W}(\widehat{f})(w)\cdot\mathrm{W}(\widehat{\mathrm{p}}_v)(u+w) = \mathrm{W}(\widehat{f})(u+v)$$

V součtu totiž dostaneme nenulovou hodnotu pouze pro $u+w=v$. Tedy $\mathrm{W}(\widehat{f+\mathrm{p}_v}) = \mathrm{W}(\widehat{f})\circ\tau_v$.

Definice. Pro booleovskou funkci $f:\mathbb{F}_2^n\to\mathbb{F}_2^m$ definujeme *korelační matici* C^f jako matici typu $2^m\times 2^n$ nad $\mathbb{R}$, kde pro $u\in\mathbb{F}_2^m$ a $v\in\mathbb{F}_2^n$ je $\mathrm{C}^f_{u,v} = \mathrm{C}(\mathrm{p}_u\circ f,\mathrm{p}_v)$.

Platí $\widehat{\mathrm{p}_u\circ f} = \sum_{v\in\mathbb{F}_2^n}\mathrm{C}^f_{u,v}\cdot\widehat{\mathrm{p}}_v$. Můžeme tedy říci, že v u-tém řádku C^f je zapsáno spektrum binární booleovské funkce $\mathrm{p}_u\circ f$. První řádek a sloupec C^f jsou indexovány nulovými vektory. V prvním řádku je tedy spektrum funkce $\mathrm{p}_0\circ f = \mathrm{p}_0$. To znamená, že v levém horním rohu C^f je hodnota 1 a zbytek prvního řádku je nulový.

Označme $\mathrm{L}_n:\mathbb{F}_2^n\to\mathbb{R}^{2^n}$ zobrazení, které vektoru $v\in\mathbb{F}_2^n$ přiřadí funkci $\widehat{\mathrm{p}}_v$.

Lemma. Pro $f:\mathbb{F}_2^n\to\mathbb{F}_2^m$ uvažme následující diagram zobrazení:

$$\begin{array}{ccc} \mathbb{F}_2^n & \xrightarrow{\ f\ } & \mathbb{F}_2^m \\ \downarrow{\scriptstyle \mathrm{L}_n} & & \downarrow{\scriptstyle \mathrm{L}_m} \\ \mathbb{R}^{2^n} & \xrightarrow{\ \mathrm{C}^f\ } & \mathbb{R}^{2^m} \end{array}$$

Tento diagram vždy komutuje, tedy $\mathrm{L}_m \circ f = \mathrm{C}^f \circ \mathrm{L}_n$. Navíc platí, že C^f je jediné lineární zobrazení, kterým lze diagram takto doplnit.

Důkaz. Korelační matici C^f můžeme chápat jako lineární zobrazení $\mathbb{R}^{2^n} \to \mathbb{R}^{2^m}$, $h \mapsto \mathrm{C}^f \cdot h$. Připomeňme, že dříve popsaným způsobem ztotožňujeme vektory $\mathbb{R}^{2^n}$ se zobrazeními $\mathbb{F}_2^n \to \mathbb{R}$. Pro $v \in \mathbb{F}_2^n$ je $(\mathrm{L}_m \circ f)(v) = \widehat{\mathrm{p}}_{f(v)}$ a $(\mathrm{C}^f \circ \mathrm{L}_n)(v) = \mathrm{C}^f \cdot \widehat{\mathrm{p}}_v$. Pro $u \in \mathbb{F}_2^m$ porovnejme u-té složky obou obrazů:

$$\begin{aligned}
\left(\widehat{\mathrm{p}}_{f(v)}\right)_u &= \widehat{\mathrm{p}}_{f(v)}(u) \\
\left(\mathrm{C}^f \cdot \widehat{\mathrm{p}}_v\right)_u &= \sum_{w \in \mathbb{F}_2^n} \mathrm{C}^f_{u,w} \cdot \widehat{\mathrm{p}}_v(w) \\
&= \sum_{w \in \mathbb{F}_2^n} \mathrm{C}(\mathrm{p}_u \circ f, \mathrm{p}_w) \cdot \widehat{\mathrm{p}}_w(v) \\
&= \left(\sum_{w \in \mathbb{F}_2^n} \mathrm{C}(\mathrm{p}_u \circ f, \mathrm{p}_w) \cdot \widehat{\mathrm{p}}_w \right)(v) \\
&= \widehat{\mathrm{p}_u \circ f}\,(v) \\
&= \widehat{\mathrm{p}}_u(f(v))
\end{aligned}$$

Zbývá dokázat jednoznačnost. Máme-li $M : \mathbb{R}^{2^n} \to \mathbb{R}^{2^m}$ doplnění na komutativní diagram, musí platit $M(\mathrm{L}_n(v)) = \mathrm{L}_m(f(v))$ pro každé $v \in \mathbb{F}_2^n$. Každá dvě doplnění na komutativní diagram se tedy na obrazu L_n shodují. Obraz L_n je přitom (ortogonální) báze $\mathbb{R}^{2^n}$. Tím získáváme jednoznačnost lineárního doplnění. □

Věta. Pro booleovské funkce $\mathbb{F}_2^n \xrightarrow{f} \mathbb{F}_2^m \xrightarrow{g} \mathbb{F}_2^k$ platí $\mathrm{C}^{g \circ f} = \mathrm{C}^g \cdot \mathrm{C}^f$.

Důkaz. Můžeme sestavit diagram zobrazení:

$$\begin{array}{ccccc}
\mathbb{F}_2^n & \xrightarrow{f} & \mathbb{F}_2^m & \xrightarrow{g} & \mathbb{F}_2^k \\
\downarrow{\scriptstyle \mathrm{L}_n} & & \downarrow{\scriptstyle \mathrm{L}_m} & & \downarrow{\scriptstyle \mathrm{L}_k} \\
\mathbb{R}^{2^n} & \xrightarrow{\mathrm{C}^f} & \mathbb{R}^{2^m} & \xrightarrow{\mathrm{C}^g} & \mathbb{R}^{2^k}
\end{array}$$

Oba čtverce v diagramu komutují, totéž tedy platí i pro jeho obvod:

$$\mathrm{L}_k \circ g \circ f = \mathrm{C}^g \circ \mathrm{L}_m \circ f = \mathrm{C}^g \circ \mathrm{C}^f \circ \mathrm{L}_n$$

Zároveň musí platit $\mathrm{L}_k \circ (g \circ f) = \mathrm{C}^{g \circ f} \circ \mathrm{L}_n$. Z jednoznačnosti lineárního doplnění plyne:

$$\mathrm{C}^{g \circ f} = \mathrm{C}^g \circ \mathrm{C}^f = \mathrm{C}^g \cdot \mathrm{C}^f$$

□

Lemma. Pro $g, h \in \mathrm{R}_n$ a bijekci $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ platí $\mathrm{C}(g \circ f, h) = \mathrm{C}(g\,, h \circ f^{-1})$.

Důkaz. Hodnoty korelace jsou dány velikostí množin $\{g \circ f = h\} = \{u \in \mathbb{F}_2^n\,;\, (g \circ f)(u) = h(u)\}$ a $\{g = h \circ f^{-1}\} = \{v \in \mathbb{F}_2^n\,;\, g(v) = (h \circ f^{-1})(v)\}$. Zobrazení $\{g \circ f = h\} \xrightarrow{f} \{g = h \circ f^{-1}\}$ a $\{g = h \circ f^{-1}\} \xrightarrow{f^{-1}} \{g \circ f = h\}$ jsou inverzní bijekce těchto množin. □

Následující věta charakterizuje booleovské permutace.

Věta. Následující podmínky jsou pro $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ ekvivalentní:

1) f je bijekce
2) C^f je ortogonální
3) C^f je invertibilní
4) $\mathrm{p}_u \circ f$ je balancovaná pro každé $0 \neq u \in \mathbb{F}_2^n$

Důkaz. Je-li f bijekce, pak podle předchozího lemmatu platí $\mathrm{C}^f_{u,v} = \mathrm{C}^{f^{-1}}_{v,u}$, tedy $\mathrm{C}^{f^{-1}} = (\mathrm{C}^f)^\top$. Zároveň je $\mathrm{C}^{f^{-1}} \cdot \mathrm{C}^f = \mathrm{C}^{f^{-1} \circ f} = \mathrm{C}^{\mathrm{Id}} = \mathrm{Id}$. Dostali jsme $(\mathrm{C}^f)^{-1} = \mathrm{C}^{f^{-1}} = (\mathrm{C}^f)^\top$, tedy platí implikace 1) $\Rightarrow$ 2).
Zřejmě platí 2) $\Rightarrow$ 3). Je-li dále korelační matice C^f invertibilní, pak je složení $\mathrm{C}^f \circ \mathrm{L}_n$ prosté zobrazení (L_n je prosté). Z rovnosti $\mathrm{L}_n \circ f = \mathrm{C}^f \circ \mathrm{L}_n$ pak musí být f prosté a tedy bijekce. Dokázali jsme ekvivalenci prvních tří podmínek.
Všechny řádky i sloupce ortogonální matice mají normu 1. Víme, že $\mathrm{C}^f_{0,0} = 1$. Pro C^f ortogonální pak musí být zbylé hodnoty prvního sloupce nulové, tedy $\mathrm{C}(\mathrm{p}_u \circ f, \mathrm{p}_0) = 0$ pro $0 \neq u \in \mathbb{F}_2^n$. Pro nenulová u jsou v tomto případě funkce $\mathrm{p}_u \circ f$ balancované.
Naopak, z podmínky 4) odvodíme ortogonalitu C^f. Pro $u, v \in \mathbb{F}_2^n$:

$$\begin{aligned}
\sum_{w \in \mathbb{F}_2^n} \mathrm{C}^f_{u,w} \cdot \mathrm{C}^f_{v,w} &= \sum_{w \in \mathbb{F}_2^n} \mathrm{W}(\widehat{\mathrm{p}_u \circ f})(w) \cdot \mathrm{W}(\widehat{\mathrm{p}_v \circ f})(w) \\
&= \left(\mathrm{W}(\widehat{\mathrm{p}_u \circ f}) \otimes \mathrm{W}(\widehat{\mathrm{p}_v \circ f})\right)(0) \\
&= \mathrm{W}(\widehat{\mathrm{p}_u \circ f + \mathrm{p}_v \circ f})(0) \\
&= \mathrm{C}(\mathrm{p}_u \circ f + \mathrm{p}_v \circ f,\, \mathrm{p}_0) \\
&= \mathrm{C}(\mathrm{p}_{u+v} \circ f,\, \mathrm{p}_0)
\end{aligned}$$

Z předpokladu je hodnota $\mathrm{C}(\mathrm{p}_{u+v} \circ f,\, \mathrm{p}_0)$ pro $u \neq v$ nulová. Pro $u = v$ je rovna jedné. Dokázali jsme, že řádky C^f tvoří ortonormální bázi $\mathbb{R}^{2^n}$. □

Na binární booleovské funkce se můžeme dívat také jako na binární náhodné veličiny. Tento pohled již přirozeným způsobem používáme - korelace funkcí f a g je určena pravděpodobnostní mírou jevu $f = g$. V tomto případě jde o náhodné veličiny s konečným obrazem. Některá tvrzení platí obecněji pro *diskrétní náhodné veličiny*, tedy náhodné veličiny s nejvýše spočetným obrazem. Budou nás tedy zajímat náhodné veličiny $X : \Omega \to G$, kde Ω je pravděpodobnostní prostor a G je nejvýše spočetný měřitelný prostor. Nejdříve připomeňme pojem vzájemné nezávislosti náhodných veličin.

Definice. Jevy $A_1, \ldots, A_k$ jsou *vzájemně nezávislé*, pokud pro každou $I \subseteq \{1, \ldots, k\}$ platí

$$\mathrm{P}\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} \mathrm{P}\left(A_i\right)$$

Definice. Diskrétní náhodné veličiny $X_1, \ldots, X_k : \Omega \to G$ jsou *vzájemně nezávislé*, pokud pro každá $b_1, \ldots, b_k \in G$ jsou jevy $X_1 = b_1, \ldots, X_k = b_k$ vzájemně nezávislé.

Lemma. Ať jsou $X_1, \ldots, X_k : \Omega \to G$ náhodné veličiny, G je nejvýše spočetný měřitelný prostor s grupovou operací $(G, +)$. Jsou-li $X_1, \ldots, X_k$ vzájemně nezávislé, pak jsou veličiny $X_1 + \cdots + X_{k-1}$ a X_k nezávislé.

Důkaz. Součet náhodných veličin definujeme obvyklým způsobem po bodech: $(X+Y)(a) = X(a)+Y(a)$. Pro $b, c \in G$ pak dostáváme:

$$\begin{aligned}
&\mathrm{P}\left((X_1+\cdots+X_{k-1}=b)\cap(X_k=c)\right) = \\
&\qquad = \mathrm{P}\left(\left(\bigsqcup_{\substack{b_1,\ldots,b_{k-1}\in G\\ b_1+\cdots+b_{k-1}=b}} (X_1=b_1)\cap\cdots\cap(X_{k-1}=b_{k-1})\right)\cap(X_k=c)\right) \\
&\qquad = \mathrm{P}\left(\bigsqcup_{\substack{b_1,\ldots,b_{k-1}\in G\\ b_1+\cdots+b_{k-1}=b}} (X_1=b_1)\cap\cdots\cap(X_{k-1}=b_{k-1})\cap(X_k=c)\right) \\
&\qquad = \sum_{\substack{b_1,\ldots,b_{k-1}\in G\\ b_1+\cdots+b_{k-1}=b}} \mathrm{P}\left((X_1=b_1)\cap\cdots\cap(X_{k-1}=b_{k-1})\cap(X_k=c)\right) \\
&\qquad = \sum_{\substack{b_1,\ldots,b_{k-1}\in G\\ b_1+\cdots+b_{k-1}=b}} \left(\prod_{i=1}^{k-1}\mathrm{P}(X_i=b_i)\right)\cdot\mathrm{P}(X_k=c) \\
&\qquad = \left(\sum_{\substack{b_1,\ldots,b_{k-1}\in G\\ b_1+\cdots+b_{k-1}=b}} \prod_{i=1}^{k-1}\mathrm{P}(X_i=b_i)\right)\cdot\mathrm{P}(X_k=c) \\
&\qquad = \mathrm{P}(X_1+\cdots+X_{k-1}=b)\cdot\mathrm{P}(X_k=c)
\end{aligned}$$

Symbolem $\bigsqcup$ zde značíme disjunktní sjednocení. □

Pro předchozí důkaz stačí předpoklad, že $(G,+)$ je pologrupa. V našem případě bude $(G,+)$ dvouprvková grupa.

Lemma (*Piling-up*). Pro $f_1,\ldots,f_k \in \mathrm{R}_n$ vzájemně nezávislé náhodné veličiny platí

$$\mathrm{C}(f_1+\cdots+f_k,0) = \prod_{i=1}^{k}\mathrm{C}(f_i,0)$$

Důkaz. Postupujme indukcí podle k. Pro $k=1$ tvrzení platí, pro $k=2$:

$$\begin{aligned}
\mathrm{C}(f+g,0) &= \mathrm{C}(f,g) \\
&= 2\cdot\mathrm{P}(f=g)-1 \\
&= 2\cdot\mathrm{P}(((f=0)\cap(g=0))\sqcup((f=1)\cap(g=1)))-1 \\
&= 2\cdot(\mathrm{P}(f=0)\cdot\mathrm{P}(g=0)+\mathrm{P}(f=1)\cdot\mathrm{P}(g=1))-1 \\
&= 2\cdot(\mathrm{P}(f=0)\cdot\mathrm{P}(g=0)+(1-\mathrm{P}(f=0))\cdot(1-\mathrm{P}(g=0)))-1 \\
&= 4\cdot\mathrm{P}(f=0)\cdot\mathrm{P}(g=0)-2\cdot\mathrm{P}(f=0)-2\cdot\mathrm{P}(g=0)+1 \\
&= (2\cdot\mathrm{P}(f=0)-1)\cdot(2\cdot\mathrm{P}(g=0)-1)
\end{aligned}$$

Předpokládejme, že pro méně než k funkcí tvrzení platí. Z předpokladu plyne, že $f_1+\cdots+f_{k-1}$ a f_k jsou nezávislé, tedy:

$$\mathrm{C}((f_1 + \cdots + f_{k-1}) + f_k, 0) = \mathrm{C}(f_1 + \cdots + f_{k-1}, 0) \cdot \mathrm{C}(f_k, 0) = \left(\prod_{i=1}^{k-1} \mathrm{C}(f_i, 0) \right) \cdot \mathrm{C}(f_k, 0)$$

□

Ve zbytku tohoto textu popíšeme tvary korelačních matic vrstev kola substitučně-permutační sítě. Víme, že korelační matice celého kola SPN pak bude - pro konkrétní hodnoty kolových klíčů - součinem korelačních matic jednotlivých vrstev. Později ukážeme, jak i bez znalosti konkrétních kolových klíčů využít tvar této matice při lineárním útoku na SPN.

Začneme jednoduššími případy přičtení klíče a permutační vrstvy.

Přičtení klíče

Pro klíč $K \in \mathbb{F}_2^n$ jde o korelační matici posunutí $\tau_K : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Pro $u, w \in \mathbb{F}_2^n$ platí:

$$\mathrm{p}_u \circ \tau_K(w) = \mathrm{p}_u(w + K) = \mathrm{p}_u(w) + \mathrm{p}_u(K) = \mathrm{p}_u(w) + u \cdot K = (\mathrm{p}_u + \mathrm{const}_{u \cdot K})(w)$$

Tedy

$$\mathrm{C}^{\tau_K}_{u,v} = \mathrm{C}(\mathrm{p}_u \circ \tau_K, \mathrm{p}_v) = \mathrm{C}(\mathrm{p}_u + \mathrm{const}_{u \cdot K}, \mathrm{p}_v) = \mathrm{C}(\mathrm{p}_{u+v}, \mathrm{const}_{u \cdot K})$$

Je-li $u = v$, pak $\mathrm{C}^{\tau_K}_{u,v} = (-1)^{u \cdot K}$. V opačném případě je $\mathrm{C}^{\tau_K}_{u,v} = 0$, neboť nenulové parity jsou balancované.
Korelační matice přičtení klíče je tedy diagonální matice, na diagonále jsou hodnoty ± 1. Složíme-li přičtení klíče s booleovskou funkcí g, korelační matice složení $\mathrm{C}^{g \circ \tau_K} = \mathrm{C}^g \cdot \mathrm{C}^{\tau_K}$ vznikne vynásobením některých sloupců (v opačném pořadí složení řádků) C^g hodnotou -1.

Permutační vrstva

Permutace složek je speciální případ lineární bijekce. Pro lineární funkci $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a $u \in \mathbb{F}_2^n$ je $\mathrm{p}_u \circ f$ opět lineární. V každém řádku C^f je tedy právě jedna jednička ($\mathrm{C}^f_{u,v} = 1$ pro $\mathrm{p}_u \circ f = \mathrm{p}_v$), jinak nuly. Je-li f navíc bijekce, je C^f permutační matice (rovnost $\mathrm{p}_u \circ f = \mathrm{p}_{u'} \circ f$ implikuje $\mathrm{p}_u = \mathrm{p}_{u'}$). Pro permutaci složek pak platí $\mathrm{p}_{f(v)} \circ f = \mathrm{p}_v$.
Složíme-li lineární bijekci f s booleovskou funkcí g, korelační matice složení $\mathrm{C}^{g \circ f}$ vznikne permutací sloupců (v opačném pořadí složení řádků) C^g.

Vrstva S*-boxů*

Konkatenaci S-boxů můžeme popsat jako kartézský součin. Obecněji, mějme booleovské funkce $f_i : \mathbb{F}_2^{n_i} \to \mathbb{F}_2^{l_i}$, $i = 1, \ldots, m$. Tyto funkce indukují zobrazení kartézských součinů

$$f : \mathbb{F}_2^n \to \mathbb{F}_2^l, \text{ kde } n = \sum_{i=1}^{m} n_i \,, \; l = \sum_{i=1}^{m} l_i$$

Vektor $w \in \mathbb{F}_2^n$ můžeme zapsat jako

$$w = (w^{(1)} | \ldots | w^{(m)}), \; w^{(i)} \in \mathbb{F}_2^{n_i}$$

a jeho obraz

$$f(w) = (f_1(w^{(1)}) | \ldots | f_m(w^{(m)})) \in \mathbb{F}_2^l$$

Takto zkonstruovaná booleovská funkce f se nazývá *bricklayer funkce*. Pro hodnoty korelační matice bricklayer funkce platí:

$$\mathrm{C}^{f}_{u,v} = \prod_{i=1}^{m} \mathrm{C}^{f_i}_{u^{(i)},v^{(i)}}$$

Před důkazem tohoto tvrzení zaveďme funkce $\tilde{f}_i : \mathbb{F}_2^n \to \mathbb{F}_2^{l_i}$ jako složení příslušné projekce s f_i:

$$\begin{array}{ccc} \mathbb{F}_2^n & \twoheadrightarrow & \mathbb{F}_2^{n_i} \\ & \searrow^{\tilde{f}_i} & \downarrow{\scriptstyle f_i} \\ & & \mathbb{F}_2^{l_i} \end{array}$$

a podobně pro $v \in \mathbb{F}_2^n$ funkce $\tilde{\mathrm{p}}_{v,i}$:

$$\begin{array}{ccc} \mathbb{F}_2^n & \twoheadrightarrow & \mathbb{F}_2^{n_i} \\ & \searrow^{\tilde{\mathrm{p}}_{v,i}} & \downarrow{\scriptstyle \mathrm{p}_{v^{(i)}}} \\ & & \mathbb{F}_2 \end{array}$$

Pro $u \in \mathbb{F}_2^l$ a $v \in \mathbb{F}_2^n$ pak platí

$$\mathrm{p}_u \circ f = \sum_{i=1}^{m} \mathrm{p}_{u^{(i)}} \circ \tilde{f}_i \quad , \quad \mathrm{p}_v = \sum_{i=1}^{m} \tilde{\mathrm{p}}_{v,i}$$

Dokažme, že pro $u \in \mathbb{F}_2^l$ a $v \in \mathbb{F}_2^n$ jsou náhodné veličiny $\tilde{g}_i = \mathrm{p}_{u^{(i)}} \circ \tilde{f}_i + \tilde{\mathrm{p}}_{v,i}$, $i = 1, \ldots, m$, vzájemně nezávislé. Opět máme komutativní diagram:

$$\begin{array}{ccc} \mathbb{F}_2^n & \twoheadrightarrow & \mathbb{F}_2^{n_i} \\ & \searrow^{\tilde{g}_i} & \downarrow{\scriptstyle g_i = \mathrm{p}_{u^{(i)}} \circ f_i + \mathrm{p}_{v^{(i)}}} \\ & & \mathbb{F}_2 \end{array}$$

K důkazu vzájemné nezávislosti $\tilde{g}_i$ využijeme pouze fakt, že hodnoty těchto funkcí závisí na disjunktních množinách indexů $\mathbb{F}_2^n$. Pro $b \in \mathbb{F}_2$ platí:

$$\mathrm{P}(\tilde{g}_i = b) = \frac{|\, \tilde{g}_i = b \,|}{2^n} = \frac{2^{n-n_i} \cdot |\, g_i = b \,|}{2^n} = \frac{|\, g_i = b \,|}{2^{n_i}} = \mathrm{P}(g_i = b)$$

Zvolme $b_1, \ldots, b_m \in \mathbb{F}_2$ a $I \subseteq \{1, \ldots, m\}$:

$$\mathrm{P}\left(\bigcap_{i \in I} (\tilde{g}_i = b_i)\right) = \frac{1}{2^n} \cdot \left(2^{n - \sum_{i \in I} n_i} \cdot \prod_{i \in I} |\, g_i = b_i \,|\right) =$$

$$= \prod_{i \in I} \frac{|\, g_i = b_i \,|}{2^{n_i}} = \prod_{i \in I} \mathrm{P}(g_i = b_i) = \prod_{i \in I} \mathrm{P}(\tilde{g}_i = b_i)$$

Nyní můžeme odvodit hodnoty korelační matice C^f:

$$\mathrm{C}^f_{u,v} \;=\; \mathrm{C}(\mathrm{p}_u{}^\circ f, \mathrm{p}_v) \;=\; \mathrm{C}(\mathrm{p}_u{}^\circ f + \mathrm{p}_v, 0) \;=\; \mathrm{C}\left(\sum_{i=1}^{m} \mathrm{p}_{u^{(i)}}{}^\circ \tilde{f}_i + \tilde{\mathrm{p}}_{v,i}\,, 0\right) \;=$$

$$= \prod_{i=1}^{m} \mathrm{C}(\mathrm{p}_{u^{(i)}}{}^\circ \tilde{f}_i + \tilde{\mathrm{p}}_{v,i}\,, 0) \;=\; \prod_{i=1}^{m} \mathrm{C}\left(\mathrm{p}_{u^{(i)}}{}^\circ f_i + \mathrm{p}_{v^{(i)}}, 0\right) \;=\; \prod_{i=1}^{m} \mathrm{C}^{f_i}_{u^{(i)},v^{(i)}}$$