A PROOF OF STRASSEN’S SEMIRING THEOREM

Notes for our seminar — Lex Schrijver

Fix a commutative semiring \((S,+,\cdot)\); so \((S,+)\) is an additive commutative semigroup with null 0 and \((S,\cdot)\) is a multiplicative commutative semigroup with unit 1, satisfying \(0a = 0\) and \(a(b+c) = ab + ac\) for all \(a, b, c \in S\). As usual, for any \(n \in \mathbb{N}\), the \(n\)-fold sum of 1 is denoted by \(n\).

Call a preorder \(\leq\) on \(S\) good if for all \(a, b, c \in S\):

1. \(n \leq n + 1\) and \(n + 1 \leq n\) for all \(n \in \mathbb{N}\);
2. if \(a \leq b\), then \(a + c \leq b + c\) and \(ac \leq bc\);
3. if \(b \neq 0\), then \(a \leq nb\) for some \(n \in \mathbb{N}\).

Note that (i) says that \(\leq\) induces the natural total order on \(\mathbb{N}\). Note also that \(0 \leq c\) for all \(c \in S\) (by (ii), as \(0 \leq 1\)).

For any good preorder \(\leq\), Volker Strassen [6] defines the asymptotic order \(\preceq\) associated with \(\leq\) by, for \(a, b \in S\):

\[
\forall r : \mathbb{N} \rightarrow \mathbb{N} \forall n \in \mathbb{N}: a^n \leq r(n)b^n \text{ and } \inf_{n \geq 1} r(n)^{1/n} = 1.
\]

Clearly, \(a \leq b\) implies \(a \preceq b\) (as then we can take \(r(1) = 1\)). Since for \(r\) in [2] one has \(a^{n+m} \leq r(n)r(m)b^{n+m}\) for all \(n, m\), we can assume that \(r(n+m) \leq r(n)r(m)\). Hence, by Fekete’s lemma [4], we can assume that \(\lim_{n \to \infty} r(n)^{1/n} = 1\).

Strassen [6] proved, using the Kadison-Dubois theorem ([5], [2,3], cf. [1]).

**Strassen’s semiring theorem.** Let \(\preceq\) be a good preorder. Then for all \(a, b \in S\): \(a \preceq b\) if and only if \(\varphi(a) \leq \varphi(b)\) for each monotone homomorphism \(\varphi : S \rightarrow \mathbb{R}_+\).

We give five propositions, from which Strassen’s theorem will be derived.

**Proposition 1.** \(\preceq\) is a good preorder.

**Proof.** Trivially, \(\leq\) is a preorder containing \(\leq\). So (1)(iii) for \(\preceq\) is direct. To prove that \(\preceq\) is good, we prove (1)(i) and (ii) for \(\preceq\).

Let \(a, b \in S\) with \(a \preceq b\). So there exists \(r : \mathbb{N} \rightarrow \mathbb{N}\) satisfying \(\lim_{n \to \infty} r(n)^{1/n} = 1\) and \(a^n \leq r(n)b^n\) for all \(n \in \mathbb{N}\). We can assume that \(r\) is nondecreasing. Then for any \(c \in S\):

\[
(a + c)^n = \sum_{k=0}^{n} \binom{n}{k} a^k c^{n-k} \leq \sum_{k=0}^{n} \binom{n}{k} r(k) b^k c^{n-k} \leq \sum_{k=0}^{n} \binom{n}{k} r(n) b^k c^{n-k} = r(n)(b + c)^n.
\]

So \(a + c \preceq b + c\). Moreover,

---

1. If \(c_1, c_2, \ldots \in \mathbb{R}_+\) with \(\inf_n c_n = 0\) for all \(n, m \in \mathbb{N}\), then \(\lim_{n \to \infty} c_n^{1/n} = \inf_{n \geq 1} c_n^{1/n}\).

2. A function \(\varphi : S \rightarrow \mathbb{R}_+\) is a monotone homomorphism if for all \(a, b \in S\): \(\varphi(a + b) = \varphi(a) + \varphi(b)\), \(\varphi(ab) = \varphi(a)\varphi(b)\), \(\varphi(1) = 1\), and, if \(a \leq b\), then \(\varphi(a) \leq \varphi(b)\).

3. Define \(r'(n) := \max_{k \leq n} r(k)\). Then \(a^n \leq r(n)b^n \leq r'(n)b^n\) for each \(n\). To show \(\lim_{n \to \infty} r'(n)^{1/n} = 1\), choose a real \(\gamma > 1\). Choose \(N\) with \(r(k)^{1/k} < \gamma\) for all \(k \geq N\). Choose \(K \geq N\) with \(r(k)^{1/k} < \gamma\) for all \(k < N\). (This is possible, since there are only finitely many \(k < N\).) Then \(r'(n)^{1/n} < \gamma\) for all \(n \geq K\). Indeed, \(r'(n) = r(k)\) for some \(k \leq n\). If \(k < N\), then \(r'(n)^{1/n} = r(k)^{1/n} \leq r(k)^{1/k} < \gamma\) (since \(n \geq K\) and \(k < N\)). If \(k \geq N\), then \(r'(n)^{1/n} = r(k)^{1/n} \leq r(k)^{1/k} < \gamma\) (since \(n \geq k\) and \(k \geq N\)).
\[(ac)^n = a^n c^n \leq r(n)b^n c^n = r(n)(bc)^n.\]

So \(ac \leq bc\). This proves (1)(ii) for \(\preceq\).

To check (1)(i), let \(a\) and \(b\) belong in particular to \(\mathbb{N}\) and \(a = b + 1\). Then, by taking \(n\)-th roots, \(a^n \leq r(n)b^n\) gives \(b + 1 = a \leq \inf_{n \geq 1} r(n)^{1/n}b = b\), contradicting (1)(i) for \(\leq\). So (1)(i) holds for \(\preceq\).

Call a preorder \(\leq\) **closed** if \(\leq\) is good and \(\preceq\) is equal to \(\leq\).

**Proposition 2.** \(\preceq\) is closed.

**Proof.** Let \(a, b \in S\) with \(a \preceq b\). So there exists \(r : \mathbb{N} \to \mathbb{N}\) satisfying \(\inf_{n \geq 1} r(n)^{1/n} = 1\) and \(a^n \preceq r(n)b^n\) for all \(n\). We must show that \(a \preceq b\).

It is enough to prove that, for any real \(\gamma > 1\), there exist \(k, t \in \mathbb{N}\) with \(k \geq 1\), \(t^{1/k} < \gamma\), and \(a^k \leq tb^k\). To that end, choose \(n \geq 1\) with \(r(n)^{1/n} < \sqrt{k}\). As \(a^n \preceq r(n)b^n\), by definition of \(\preceq\) there exists \(s : \mathbb{N} \to \mathbb{N}\) with \(\inf_{m \geq 1} s(m)^{1/m} = 1\) and \((a^n)m \leq s(m)(r(n)b^n)m\) for all \(m\). Choose \(m \geq 1\) with \(s(m)^{1/m} < \sqrt{k}\). Then for \(k := nm\) and \(t := s(m)r(n)^m\) one has \(a^k = a^{nm} \leq s(m)r(n)^mb^{nm} = tb^{nm} = tb^k\) and \(t^{1/k} = t^{1/nm} = s(m)^{1/nm}r(n)^{1/n} < \gamma\), as required.

**Proposition 3.** Let \(\leq\) be closed. Then for all \(a, b, c \in S\):

\[(5) \quad (i) \text{ if } a + c \leq b + c, \text{ then } a \leq b;\]
\[(ii) \text{ if } ac \leq bc \text{ and } c \neq 0, \text{ then } a \leq b;\]
\[(iii) \text{ if } na \leq nb + 1 \text{ for all } n \in \mathbb{N}, \text{ then } a \leq b.\]

**Proof.** I. First we prove (5)(ii). Assume \(ac \leq bc\) and \(c \neq 0\). Induction gives \(a^n c \leq b^n c\) for each \(n \in \mathbb{N}\), since \(a^0c = b^0c\) and \(a^{n+1}c = a^nac \leq a^nbc \leq b^nbc = b^{n+1}c\).

By (1)(iii), there exist \(r, k \in \mathbb{N}\) with \(1 \leq cr \leq k\). Then \(a^n \leq a^n cr \leq b^n cr \leq kb^n\) for each \(n \in \mathbb{N}\). As \(\inf_{n \geq 1} k^{1/n} = 1\), we know \(a \preceq b\), hence, as \(\preceq\) is equal to \(\leq\), \(a \leq b\).

II. Next we prove (5)(iii). Assume \(na \leq 1 + nb\) for each \(n \in \mathbb{N}\). If \(b = 0\), then \(a = 0\) by (1)(iii), hence \(a \preceq b\). So we can assume \(b \neq 0\). Let \(r \in \mathbb{N}\) satisfy \(1 \leq rb\). So for all \(n \in \mathbb{N}\) we have \(na \leq nb + 1 \leq (n + r)b\). Consider any \(k \in \mathbb{N}\), and choose \(n\) large enough such that \((n + r)^k \leq 2nk\). Then \(n^k a^k \leq (n + r)^k b^k \leq 2nk b^k\). Hence by (5)(ii), \(a^k \leq 2b^k\). As this holds for each \(k \in \mathbb{N}\) and as \(\inf_{k \geq 1} 2^{1/k} = 1\), we know \(a \preceq b\). Hence, as \(\preceq\) is equal to \(\leq\), \(a \leq b\).

III. Finally, we prove (5)(i). Assume \(a + c \leq b + c\). Induction gives \(na + c \leq nb + c\) for each \(n \in \mathbb{N}\), since \(0a + c = 0b + c\) and \((n + 1)a + c = na + a + c \leq na + b + c \leq nb + b + c = (n + 1)b + c\).

Choose \(k \in \mathbb{N}\) with \(c \leq k\). Then \(na \leq na + c \leq nb + c \leq nb + k\) for each \(n \in \mathbb{N}\). Replacing \(n\) by \(nk\), we get \(nka \leq nk(b + k)\), for each \(n \in \mathbb{N}\). So by (5)(ii), \(na \leq nb + 1\) for each \(n \in \mathbb{N}\). Hence by (5)(iii), \(a \leq b\).

**Proposition 4.** Let \(\leq\) be closed and \(a \not\leq b\). Then there exists a good preorder \(\preceq\) containing \(\leq\) and satisfying \(b \preceq a\).

**Proof.** Define \(\leq\) by, for \(x, y \in S\),

\[(6) \quad x \leq y \iff \exists c \in S: x + ac \leq y + bc.\]
Then $\leq$ contains $\preceq$, since if $x \preceq y$, then $x + a0 \leq y + b0$, so $x \leq y$. Also, $b \preceq a$, since $b + a1 = a + b1$. As $\leq$ contains $\preceq$, the relation $\leq$ is reflexive and satisfies (4)(iii).

To see that $\leq$ is transitive, let $x \leq y$ and $y \leq z$. Then $x + ac \leq y + bc$ and $y + ad \leq z + bd$ for some $c, d \in S$. Therefore, $x + a(c + d) \leq y + ba + ad \leq z + b(c + d)$. So $x \leq z$.

To see (4)(ii) for $\preceq$, let $x \preceq y$ and $z \in S$. Then $x + ac \leq y + bc$ for some $c \in S$, hence $x + z + ac \leq y + z + bc$ and $xz + acz \leq yz + bc$. So $x + z \preceq y + z$ and $xz \preceq yz$.

Finally, to check (4)(i) for $\preceq$, suppose that $n + 1 \leq n$ for some $n \in \mathbb{N}$. Hence $n + 1 + ac \leq n + bc$ for some $c \in S$, implying (by (5)(i)) $1 + ac \leq bc$. So $c \neq 0$ (otherwise $1 \leq 0$ would follow) and $ac \leq bc$, implying (by (5)(ii)) $a \leq b$. This contradicts $a \not\preceq b$. □

**Proposition 5.** If $\leq$ is good, there exists a monotone homomorphism $\varphi : S \rightarrow \mathbb{R}_+$. 

**Proof.** Let $\leq$ be good. By Zorn’s lemma, we can assume that $\leq$ is an inclusionwise maximal good preorder. This implies that $\preceq$ is not larger than $\leq$. So $\leq$ is closed.

For each $a \in S$, define

(7) \[ L_a := \{ \frac{k}{n} \mid k, n \in \mathbb{N}, n \geq 1, k \leq na \} \quad \text{and} \quad U_a := \{ \frac{k}{n} \mid k, n \in \mathbb{N}, n \geq 1, na \leq k \}. \]

Note that if $\frac{k}{n} = \frac{k'}{n'}$, then $k \leq na \iff k'n = kn' \leq mn'a \iff k' \leq n'a$, by (4)(ii) and (5)(ii). Similarly, $na \leq k \iff n'a \leq k'$.

Now for each $\frac{k}{n} \in L_a$ and $\frac{k'}{n'} \in U_a$ one has $\frac{k}{n} \leq \frac{k'}{n'}$, since $k \leq na$ and $n'a \leq k'$ give $kn' \leq mn'a \leq k'n$. Moreover, $L_a \cup U_a = \mathbb{Q}_+$, since for each $k, n \in \mathbb{N}$, at least one of $k \leq na$ and $na \leq k$ holds, as otherwise by Proposition 4 we can augment $\leq$ with $na \leq k$ (because $k \not\preceq na$), contradicting the maximality of $\leq$. Finally, $L_a \neq \emptyset$ and $U_a \neq \emptyset$, since $0 \leq a \leq k$ for some $k \in \mathbb{N}$, by (4)(iii).

So we can define $\varphi(a) := \inf L_a$. Consider $a, b \in S$. Then $L_{a+b} \supseteq L_a + L_b$, since if $\frac{k}{n} \in L_a$ and $\frac{k'}{n'} \in L_b$, then $k \leq na$ and $k' \leq n'b$, hence $kn' + k'n \leq mn'a + mn'b = mn'(a + b)$, so that $\frac{k}{n} + \frac{k'}{n} = \frac{kn' + k'n}{nn'}$ belongs to $L_{a+b}$. This implies $\varphi(a + b) \geq \varphi(a) + \varphi(b)$.

One similarly proves $U_{a+b} \supseteq U_a + U_b$, hence $\varphi(a + b) \leq \varphi(a) + \varphi(b)$. So $\varphi(a + b) = \varphi(a) + \varphi(b)$. Similarly, since $L_{ab} \supseteq L_a L_b$ and $U_{ab} \supseteq U_a U_b$ we have $\varphi(ab) = \varphi(a)\varphi(b)$. Finally, if $a \leq b$, then $L_a \subseteq L_b$, hence $\varphi(a) \leq \varphi(b)$. □

**Proof of Strassen’s semiring theorem.** To see necessity, let $a \preceq b$ and let $\varphi$ be a $\preceq$-monotone homomorphism. Let $r : \mathbb{N} \rightarrow \mathbb{N}$ satisfy $\inf_{a \geq 1} r(n)^{1/n} = 1$ and $a^n \leq r(n)b^n$ for all $n$. Then $\varphi(a)^n = \varphi(a^n) \leq \varphi(r(n)b^n) = r(n)\varphi(b)^n$ for all $n \in \mathbb{N}$. Taking $n$-th roots and infimum over $n$, we obtain $\varphi(a) \leq \varphi(b)$.

To see sufficiency of the condition in Strassen’s semiring theorem, we can assume that $\leq$ is closed, as the condition for $\preceq$ implies the condition for $\leq$. So $\leq$ satisfies (5).

Choose $a, b \in S$ with $a \not\preceq b$. We must prove that $\varphi(a) \not\preceq \varphi(b)$ for some monotone homomorphism $\varphi : S \rightarrow \mathbb{R}_+$.

By (5)(iii), as $a \not\preceq b$, there exists $n \in \mathbb{N}$ with $na \not\preceq 1 + nb$. Then, by Proposition 4, there exists a good preorder $\preceq$ containing $\leq$ and satisfying $1 + nb \leq na$. Next by Proposition 5 there exists a homomorphism $\varphi : S \rightarrow \mathbb{R}_+$ that is monotone with respect to $\preceq$. As $\leq$ contains $\preceq$, $\varphi$ is also monotone with respect to $\leq$. Moreover, as $1 + nb \preceq na$, we have $\varphi(1 + nb) \leq \varphi(na)$, so $1 + n\varphi(b) \leq n\varphi(a)$, yielding $\varphi(b) < \varphi(a)$, as required. □
References


