## A PROOF OF STRASSEN'S SEMIRING THEOREM

Notes for our seminar - Lex Schrijver

Fix a commutative semiring $(S,+$,$) ; so (S,+)$ is an additive commutative semigroup with null 0 and ( $S$, ) is a multiplicative commutative semigroup with unit 1 , satisfying $0 a=0$ and $a(b+c)=a b+a c$ 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 $a, b, c \in S$ :
(i) $n \leq n+1$ and $n+1 \not \leq n$ for all $n \in \mathbb{N}$;
(ii) if $a \leq b$, then $a+c \leq b+c$ and $a c \leq b c$;
(iii) if $b \neq 0$, then $a \leq n b$ 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 $\lesssim$ associated with $\leq$ by, for $a, b \in S$ :

$$
\begin{equation*}
a \lesssim b \Longleftrightarrow \exists r: \mathbb{N} \rightarrow \mathbb{N} \quad \forall n \in \mathbb{N}: a^{n} \leq r(n) b^{n} \text { and } \inf _{n \geq 1} r(n)^{1 / n}=1 \tag{2}
\end{equation*}
$$

Clearly, $a \leq b$ implies $a \lesssim b$ (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 $\lim _{n \rightarrow \infty} r(n)^{1 / n}=1$.

Strassen [6] proved, using the Kadison-Dubois theorem ([5], [2,3], cf. [1]) :2
Strassen's semiring theorem. Let $\leq b e$ a good preorder. Then for all $a, b \in S: a \lesssim b$ 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. $\lesssim$ is a good preorder.
Proof. Trivially, $\lesssim$ is a preorder containing $\leq$. So (1)(iii) for $\lesssim$ direct. To prove that $\lesssim$ is good, we prove (1)(i) and (ii) for $\lesssim$.

Let $a, b \in S$ with $a \lesssim b$. So there exists $r: \mathbb{N} \rightarrow \mathbb{N}$ satisfying $\lim _{n \rightarrow \infty} r(n)^{1 / n}=1$ and $a^{n} \leq r(n) b^{n}$ for all $n \in \mathbb{N}$. We can assume that $r$ is nondecreasing. ${ }^{3}$ Then for any $c \in S$ :

$$
\begin{equation*}
(a+c)^{n}=\sum_{k=0}^{n}\binom{n}{k} a^{k} c^{n-k} \leq \sum_{k=0}^{n}\binom{n}{k} r(k) b^{k} c^{n-k} \leq \sum_{k=0}^{n}\binom{n}{k} r(n) b^{k} c^{n-k}=r(n)(b+c)^{n} . \tag{3}
\end{equation*}
$$

So $a+c \lesssim b+c$. Moreover,

[^0]\[

$$
\begin{equation*}
(a c)^{n}=a^{n} c^{n} \leq r(n) b^{n} c^{n}=r(n)(b c)^{n} \tag{4}
\end{equation*}
$$

\]

So $a c \lesssim b c$. This proves $\sqrt{1}$ (ii) for $\lesssim$.
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 $\lesssim$.

Call a preorder $\leq$ closed if $\leq$ is good and $\lesssim$ is equal to $\leq$.
Proposition 2. $\lesssim i s ~ c l o s e d$.
Proof. Let $a, b \in S$ with $a \lesssim b$. So there exists $r: \mathbb{N} \rightarrow \mathbb{N}$ satisfying $\inf _{n \geq 1} r(n)^{1 / n}=1$ and $a^{n} \lesssim r(n) b^{n}$ for all $n$. We must show that $a \lesssim b$.

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 $a^{k} \leq t b^{k}$. To that end, choose $n \geq 1$ with $r(n)^{1 / n}<\sqrt{\gamma}$. As $a^{n} \lesssim r(n) b^{n}$, by definition of $\lesssim$ there exists $s: \mathbb{N} \rightarrow \mathbb{N}$ with $\inf _{m \geq 1} s(m)^{1 / m}=1$ and $\left(a^{n}\right)^{m} \leq s(m)\left(r(n) b^{n}\right)^{m}$ for all $m$. Choose $m \geq 1$ with $s(m)^{1 / m}<\sqrt{\gamma}$. Then for $k:=n m$ and $t:=s(m) r(n)^{m}$ one has $a^{k}=a^{n m} \leq s(m) r(n)^{m} b^{n m}=t b^{n m}=t b^{k}$ and $t^{1 / k}=t^{1 / n m}=s(m)^{1 / n m} r(n)^{1 / n}<\gamma$, as required.

Proposition 3. Let $\leq$ be closed. Then for all $a, b, c \in S$ :
(i) if $a+c \leq b+c$, then $a \leq b$;
(ii) if $a c \leq b c$ and $c \neq 0$, then $a \leq b$;
(iii) if $n a \leq n b+1$ for all $n \in \mathbb{N}$, then $a \leq b$.

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

By (1)(iii), there exist $r, k \in \mathbb{N}$ with $1 \leq c r \leq k$. Then $a^{n} \leq a^{n} c r \leq b^{n} c r \leq k b^{n}$ for each $n \in \mathbb{N}$. As $\inf _{n \geq 1} k^{1 / n}=1$, we know $a \lesssim b$, hence, as $\lesssim$ is equal to $\leq, a \leq b$.
II. Next we prove (5) (iii). Assume $n a \leq 1+n b$ for each $n \in \mathbb{N}$. If $b=0$, then $a=0$ by (1) (iii), hence $a \leq b$. So we can assume $b \neq 0$. Let $r \in \mathbb{N}$ satisfy $1 \leq r b$. So for all $n \in \mathbb{N}$ we have $n a \leq n b+1 \leq(n+r) b$. Consider any $k \in \mathbb{N}$, and choose $n$ large enough such that $(n+r)^{k} \leq 2 n^{k}$. Then $n^{k} a^{k} \leq(n+r)^{k} b^{k} \leq 2 n^{k} b^{k}$. Hence by (5)(ii), $a^{k} \leq 2 b^{k}$. As this holds for each $k \in \mathbb{N}$ and as $\inf _{k \geq 1} 2^{1 / k}=1$, we know $a \lesssim b$. Hence, as $\lesssim$ is equal to $\leq, a \leq b$.
III. Finally, we prove (5)(i). Assume $a+c \leq b+c$. Induction gives $n a+c \leq n b+c$ for each $n \in \mathbb{N}$, since $0 a+c=0 b+c$ and $(n+1) a+c=n a+a+c \leq n a+b+c \leq n b+b+c=(n+1) b+c$.

Choose $k \in \mathbb{N}$ with $c \leq k$. Then $n a \leq n a+c \leq n b+c \leq n b+k$ for each $n \in \mathbb{N}$. Replacing $n$ by $n k$, we get $n k a \leq n k b+k$, for each $n \in \mathbb{N}$. So by (5) (ii), $n a \leq n b+1$ 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 $\preceq$ by, for $x, y \in S$,

$$
\begin{equation*}
x \preceq y \Longleftrightarrow \exists c \in S: x+a c \leq y+b c . \tag{6}
\end{equation*}
$$

Then $\preceq$ contains $\leq$, since if $x \leq y$, then $x+a 0 \leq y+b 0$, so $x \preceq y$. Also, $b \preceq a$, since $b+a 1=a+b 1$. As $\preceq$ contains $\leq$, the relation $\preceq$ is reflexive and satisfies (1) (iii).

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

To see (11)(ii) for $\preceq$, let $x \preceq y$ and $z \in S$. Then $x+a c \leq y+b c$ for some $c \in S$, hence $x+z+a c \leq y+z+b c$ and $x z+a c z \leq y z+b c z$. So $x+z \preceq y+z$ and $x z \preceq y z$.

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

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 $\lesssim$ is not larger than $\leq$. So $\leq$ is closed.

For each $a \in S$, define

$$
\begin{equation*}
L_{a}:=\left\{\left.\frac{k}{n} \right\rvert\, k, n \in \mathbb{N}, n \geq 1, k \leq n a\right\} \text { and } U_{a}:=\left\{\left.\frac{k}{n} \right\rvert\, k, n \in \mathbb{N}, n \geq 1, n a \leq k\right\} \tag{7}
\end{equation*}
$$

Note that if $\frac{k}{n}=\frac{k^{\prime}}{n^{\prime}}$, then $k \leq n a \Longleftrightarrow k^{\prime} n=k n^{\prime} \leq n n^{\prime} a \Longleftrightarrow k^{\prime} \leq n^{\prime} a$, by (11 (ii) and (5)(ii). Similarly, $n a \leq k \Longleftrightarrow n^{\prime} a \leq k^{\prime}$.

Now for each $\frac{k}{n} \in L_{a}$ and $\frac{k^{\prime}}{n^{\prime}} \in U_{a}$ one has $\frac{k}{n} \leq \frac{k^{\prime}}{n^{\prime}}$, since $k \leq n a$ and $n^{\prime} a \leq k^{\prime}$ give $k n^{\prime} \leq n n^{\prime} a \leq k^{\prime} n$. Moreover, $L_{a} \cup U_{a}=\mathbb{Q}_{+}$, since for each $k, n \in \mathbb{N}$, at least one of $k \leq n a$ and $n a \leq k$ holds, as otherwise by Proposition 4 we can augment $\leq$ with $n a \leq k$ (because $k \not \leq n a)$, 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 (11)(iii).

So we can define $\varphi(a):=\sup L_{a}=\inf U_{a}$. Consider $a, b \in S$. Then $L_{a+b} \supseteq L_{a}+L_{b}$, since if $\frac{k}{n} \in L_{a}$ and $\frac{k^{\prime}}{n^{\prime}} \in L_{b}$, then $k \leq n a$ and $k^{\prime} \leq n^{\prime} b$, hence $k n^{\prime}+k^{\prime} n \leq n n^{\prime} a+n n^{\prime} b=n n^{\prime}(a+b)$, so that $\frac{k}{n}+\frac{k^{\prime}}{n^{\prime}}=\frac{k n^{\prime}+k^{\prime} n}{n n^{\prime}}$ 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 $L_{a b} \supseteq L_{a} L_{b}$ and $U_{a b} \supseteq U_{a} U_{b}$ we have $\varphi(a b)=\varphi(a) \varphi(b)$. 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 $a \lesssim b$ and let $\varphi$ be a $\leq$-monotone homomorphism. Let $r: \mathbb{N} \rightarrow \mathbb{N}$ satisfy $\inf _{n \geq 1} r(n)^{1 / n}=1$ and $a^{n} \leq r(n) b^{n}$ for all $n$. Then $\varphi(a)^{n}=\varphi\left(a^{n}\right) \leq \varphi\left(r(n) b^{n}\right)=r(n) \varphi(b)^{n}$ for all $n \in N$. 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 $\leq$ implies the condition for $\lesssim$. So $\leq$ satisfies (5).

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

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

## References

[1] E. Becker, N. Schwartz, Zum Darstellungssatz von Kadison-Dubois, Archiv der Mathematik 40 (1983) 421-428.
[2] D.W. Dubois, A note on David Harrison's theory of preprimes, Pacific Journal of Mathematics 21 (1967) 15-19.
[3] D.W. Dubois, Second note on David Harrison's theory of preprimes, Pacific Journal of Mathematics 24 (1968) 57-68.
[4] M. Fekete, Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, Mathematische Zeitschrift 17 (1923) 228-249.
[5] R.V. Kadison, A representation theory for commutative topological algebra, Memoirs of the American Mathematical Society 7 (1951), 39 pp.
[6] V. Strassen, The asymptotic spectrum of tensors, Journal für die reine und angewandte Mathematik 384 (1988) 102-152.


[^0]:    ${ }^{1}$ If $c_{1}, c_{2}, \ldots \in \mathbb{R}_{+}$with $c_{n+m} \leq c_{n} c_{m}$ for all $n, m \in \mathbb{N}$, then $\lim _{n \rightarrow \infty} c_{n}^{1 / n}=\inf _{n \geq 1} c_{n}^{1 / n}$.
    ${ }^{2}$ A function $\varphi: S \rightarrow \mathbb{R}_{+}$is a monotone homomorphism if for all $a, b \in S: \varphi(a+b)=\varphi(a)+\varphi(b)$, $\varphi(a b)=\varphi(a) \varphi(b), \varphi(1)=1$, and, if $a \leq b$, then $\varphi(a) \leq \varphi(b)$.
    ${ }^{3}$ Define $r^{\prime}(n):=\max _{k \leq n} r(k)$. Then $a^{n} \leq r(n) b^{n} \leq r^{\prime}(n) b^{n}$ for each $n$. To show $\lim _{n \rightarrow \infty} r^{\prime}(n)^{1 / n}=1$, 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 $r^{\prime}(n)^{1 / n}<\gamma$ for all $n \geq K$. Indeed, $r^{\prime}(n)=r(k)$ for some $k \leq n$. If $k<N$, then $r^{\prime}(n)^{1 / n}=r(k)^{1 / n} \leq r(k)^{1 / K}<\gamma$ (since $n \geq K$ and $k<N)$. If $k \geq N$, then $r^{\prime}(n)^{1 / n}=r(k)^{1 / n} \leq r(k)^{1 / k}<\gamma($ since $n \geq k$ and $k \geq N)$.

