Apartness on strongly regular rings

Bassel Mannaa

October 17, 2011

Definition 0.1. *The* apartness *relation # on a set S is defined as a relation that satisfy*

AP.1 $\neg x \# x$

AP.2 $x \# y \to y \# x$ [1]

AP.3 $x \# y \to x \# z \vee y \# z$

We use the symbol # to denote apartness without qualification. The set on which the apartness is defined should be obvious from the context.

Apartness can be regarded as a form of positive inequality. Thus, while apartness imply inequality the converse is not always true. For more on the apartness relation see Troelstra and van Dalen (1988).

Definition 0.2. *Let R be a commutative ring. In addition to the axioms in definition 0.1 an* apartness *relation # on R satisfies for all $w, x, y, z \in R$*

AP.4 $x + y \# w + z \to x \# w \vee y \# z$

AP.5 $xy \# wz \to x \# w \vee y \# z$

Lemma 0.3. *From* **AP.1-AP.5** *we can derive*

R.1 $x + y \# 0 \to x \# 0 \vee y \# 0$

R.2 $xy \# 0 \to x \# 0 \wedge y \# 0$

Proof. See Troelstra and van Dalen (1988)

Further more we prove the following fact

[1] This property is redundant, i.e. derivable from AP.1 and AP.3.

Lemma 0.4. *Let* $(R, \#)$ *be a commutative ring with apartness. For* $a, b \in R$

R.4 $a - b \# 0 \leftrightarrow a \# b$

Proof. ($\Rightarrow$) Rewrite $a - b \# 0$ to $a - b \# b - b$. From this by (AP.4) we get $a \# b \vee b \# b$ which by (AP.1) and $\vee$-elimination gives $a \# b$. ($\Leftarrow$) Rewrite $a \# b$ to $a - b + b \# 0 + b$. By (AP.4) we get $a - b \# 0 \vee b \# b$. Again by (AP.1) and $\vee$-elimination we get $a - b \# 0$. □

We try to motivate the definition of apartness on strongly regular rings that will follow. Let R be a strongly regular ring and let $a \in R$ be a non-unit and let c be its quasi-inverse. We have $R \cong R/(ac) \times R/(1 - ac)$. In $R/(ac)$ we have a, or rather its image, equal to 0. Hence the inequality with 0 does not necessarily hold for the images of a in all refinements of R. This suggest a definition, $a \# 0 : a$ is a unit. However, this will still be insufficient as we shall demonstrate. Consider for the same a, c the proposition $ac \# 0 \vee (1 - ac) \# 0$. In $R/(ac)$ only the right disjunct holds while in $R/(1 - ac)$ only the left one holds. However, the proposition holds in both refinements. We seek a definition of apartness on R for which this proposition hold. One way to know a priori that the above proposition hold is that the sum $ac + (1 - ac)$ is equal to 1. This relation must hold in all refinements. Generally, if the ideal generated by $\{a_i\}_{i \in I}$, for a finite I, is equal to R then we can state that $\exists i \in I \; a_i \# 0$. This lead us to the use of a boolean model in which ideals represent generalized truth values.

In brief, we choose a suitable boolean algebra B and we give an interpretation $[\![P]\!] : R^k \to B$, for each k-ary predicate P and an interpretation $[\![f]\!] : R^k \to R$ for each k-ary function symbol f. If $\phi = Pt_1...t_k$, the interpretation $[\![\phi]\!]$ then becomes the principal ideal generated by $[\![P]\!][\![t_1]\!]...[\![t_k]\!]$. For $\perp$ the interpretation $[\![\perp]\!]$ is the ideal $0B$. We define $[\![\phi_1 \vee \phi_2]\!]$ as the sum of ideals $[\![\phi_1]\!] + [\![\phi_2]\!]$. The interpretation of $P \to Q$ is $[\![\phi_1 \to \phi_2]\!] = [\![\phi_1]\!]^C + [\![\phi_2]\!]$ where for an ideal I, $I^C = \{e \in B \mid \forall c \in I \; ec = 0\}$. $[\![\exists x \; \phi]\!]$ is interpreted as the sum of ideals $\Sigma_{r \in R}[\![\phi]\!]_{(x=r)}$ and $[\![\forall x \; \phi]\!]$ as $\bigcap_{(r \in R)}[\![\phi]\!]_{(x=r)}$. In our case the only atomic proposition is of the form $x \# y$. A proof of a statement ϕ is equivalent to a proof of $[\![\phi]\!] = B$, see (Coquand, 1996).

Transfer principle If $x \# y$ holds in the topological model defined by B then it holds in R.

Note that for $x \# y$ to hold in a strongly regular ring R means that $x - y$ is a unit.

Definition 0.5 (Apartness on a strongly regular ring)**.** *Let* R *be a nontrivial strongly regular ring. Let* B *be the boolean algebra of idempotents of* R *(Halmos, 1963). Given* $x, y \in R$*, let* c *be the quasi-inverse of* $(x - y)$ *and let* $e = (x - y)c$*. We define* *the value*[2] *of* $x \# y$ *as*

$$[\![x \# y]\!] = eB$$

We denote the boolean sum $+'$, where $a +' b = a + b - 2ab$. Multiplication in the boolean algebra is the same as that of the ring.

Lemma 0.6. *The relation* $\#$ *as defined in 0.5 is an apartness relation.*

Proof. Since $[\![x \# x]\!]$ is the the ideal $0B$ then (AP.1) follows. Now for an arbitrary $z \in R$ let h be the quasi-inverse of $(x - z)$. Then $d = (x - z)h$ is an idempotent. Similarly, let b be the quasi-inverse of $(y - z)$ and let $f = (y - z)b$. We then have $x(1 - d) = z(1 - d)$ and $y(1 - f) = z(1 - f)$. Hence we have $x(1 - d)(1 - f) = y(1 - d)(1 - f)$. Since $e = (x - y)c$ then for any a such that $xa = ya$ we have $ea = 0$ and thus $e(1 - a) = e$. From this we conclude $e(1 - (1 - d)(1 - f)) = e$. But

$$1 - (1 - d)(1 - f) = 1 - 1 + d + f - df = d + f - df = d +' f +' df = d \vee f$$

Hence $e \wedge (d \vee f) = e$, i.e. $e \leq d \vee f$ and $[\![x \# y]\!] \subseteq [\![x \# z]\!] \vee [\![y \# z]\!]$. Thus the definition satisfies (AP.3). (AP.2) follows from (AP.1) and (AP.3). The proof for (AP.4) is similar.

Now given $x, y, w, z \in R$ let c, h and b be the quasi-inverses of $(xy - wz)$, $(x - w)$ and $(y - z)$ respectively. We have idempotents $e = (xy - wz)c$, $d = (x - w)h$ and $f = (y - z)b$. As before we have $x(1 - d) - w(1 - d) = 0$ and $y(1 - f) - z(1 - f) = 0$. We multiply the first by $y(1 - f)$ to get $xy(1 - d)(1 - f) - wy(1 - d)(1 - f) = 0$ and the second by $w(1 - d)$ to get $wy(1 - d)(1 - f) - wz(1 - d)(1 - f) = 0$. Hence we have $xy(1 - d)(1 - f) - wz(1 - d)(1 - f) = 0$ from this as in the case of (AP.3) we get $e \leq d \vee f$ and the definition satisfies (AP.5). □

Lemma 0.7. *Let* a, b *be elements in a nontrivial strongly regular ring* R*. If there exist* $x, y \in R$ *such that* $xa + yb = 1$*, then* $a \# 0 \vee b \# 0$ *holds.*

Proof. Let e, c be the quasi-inverses of a, b respectively. We have $ea \vee bc = ea + bc - eabc$. We can check that $1 = (xa + yb) \wedge (ea \vee bc)$ and thus $1 \in [\![a \# 0 \vee b \# 0]\!]$. □

Definition 0.8 (Apartness on power series)**.** *Let* $(R, \#)$ *be a ring with apartness and* $R[[X]]$ *the ring of power series over* R*. Two elements* $\alpha, \beta \in R[[X]]$ *are apart if* $\exists i \in \mathbb{N}\ \alpha(i) \# \beta(i)$*.*

It is easy to check that this definition satisfies the properties of apartness using the same boolean model B of lemma 0.6 and the topological interpretation of $\exists$.

[2] Value here refer to truth value, since ideals are considered generalized truth values.

Definition 0.9. *Let* $(R, \#)$ *be a commutative ring with apartness. The apartness relation can be extended to the ring of polynomials* $R[X]$ *in a natural way. For two polynomials*

$$F = \sum_{i=0}^{n} a_i X^i \text{ and } G = \sum_{i=0}^{m} b_j X^j \in R[X]$$

$F \# G$ *if* $\exists k \leq \max(m, n)\ a_k \# b_k$*, where* $\forall k > n\ a_k = 0$ *and* $\forall k > m\ b_k = 0$

References

Coquand, T., 1996. Computational content of classical logic. In: Semantics and Logics of Computation. Cambridge University Press, pp. 470–517.

Halmos, P. R., 1963. Lectures on boolean algebras. No. 1 in Van Nostrand Mathematical Studies. D. Van Nostrand Company, INC.

Troelstra, A. S., van Dalen, D., 1988. Constructivism in Mathematics: An Introduction. Vol. I and II of Studies in Logic and the Foundations of Mathematics. North-Holland.