The Incompatibility of $SD$-Efficiency and $SD$-Strategy-Proofness

Manuel Eberl

September 13, 2023

Abstract

This formalisation contains the proof that there is no anonymous and neutral Social Decision Scheme for at least four voters and alternatives that fulfils both $SD$-Efficiency and $SD$-Strategy-Proofness. The proof is a fully structured and quasi-human-readable one. It was derived from the (unstructured) SMT proof of the case for exactly four voters and alternatives by Brandl et al. [1].

Their proof relies on an unverified translation of the original problem to SMT, and the proof that lifts the argument for exactly four voters and alternatives to the general case is also not machine-checked.

In this Isabelle proof, on the other hand, all of these steps are also fully proven and machine-checked. This is particularly important seeing as a previously published informal proof of a weaker statement contained a mistake in precisely this lifting step. [2]

Contents

1 Incompatibility of SD-Efficiency and SD-Strategy-Proofness  2
  1.1 Preliminary Definitions ................................. 2
  1.2 Definition of Preference Profiles and Fact Gathering ...... 3
  1.3 Main Proof .............................................. 6
  1.4 Lifting to more than 4 agents and alternatives .......... 17
1 Incompatibility of SD-Efficiency and SD-Strategy-Proofness

theory SDS-Impossibility
imports
  Randomised-Social-Choice.SDS-Automation
  Randomised-Social-Choice.Randomised-Social-Choice
begin

1.1 Preliminary Definitions

locale sds-impossibility =
  anonymous-sds agents alts sds +
  neutral-sds agents alts sds +
  sd-efficient-sds agents alts sds +
  strategyproof-sds agents alts sds
for agents :: 'agent set and alts :: 'alt set and sds +
assumes agents-ge-4: card agents ≥ 4
and alts-ge-4: card alts ≥ 4

locale sds-impossibility-4-4 = sds-impossibility agents alts sds
for agents :: 'agent set and alts :: 'alt set and sds +
fixes A1 A2 A3 A4 :: 'agent and a b c d :: 'alt
assumes distinct-agents: distinct [A1, A2, A3, A4]
and distinct-alts: distinct [a, b, c, d]
and agents: agents = {A1, A2, A3, A4}
and alts: alts = {a, b, c, d}
begin

lemma an-sds: an-sds agents alts sds by unfold-locales
lemma ex-post-efficient-sds: ex-post-efficient-sds agents alts sds by unfold-locales
lemma sd-efficient-sds: sd-efficient-sds agents alts sds by unfold-locales
lemma strategyproof-an-sds: strategyproof-an-sds agents alts sds by unfold-locales

lemma distinct-agents' [simp]:
  A1 ≠ A2 A1 ≠ A3 A1 ≠ A4 A2 ≠ A1 A2 ≠ A3 A2 ≠ A4
  A3 ≠ A1 A3 ≠ A2 A3 ≠ A4 A4 ≠ A1 A4 ≠ A2 A4 ≠ A3
using distinct-agents by auto

lemma distinct-alts' [simp]:
  a ≠ b a ≠ c a ≠ d b ≠ a b ≠ c b ≠ d
  c ≠ a c ≠ b c ≠ d d ≠ a d ≠ b d ≠ c
using distinct-alts by auto

lemma card-agents [simp]: card agents = 4 and card-alts [simp]: card alts = 4
using distinct-agents distinct-alts by (simp-all add: agents alts)

lemma in-agents [simp]: A1 ∈ agents A2 ∈ agents A3 ∈ agents A4 ∈ agents
by (simp-all add: agents)
1.2 Definition of Preference Profiles and Fact Gathering

preference-profile
agents: agents
alts: alts
where R1 = A1: [c, d], [a, b]  A2: [b, d], a, c  A3: a, b, [c, d]  A4: [a, c], [b, d]
and R2 = A1: [a, c], [b, d]  A2: [c, d], a, b  A3: [b, d], a, c  A4: a, b,
and R3 = A1: [a, b], [c, d]  A2: [c, d], [a, b]  A3: d, [a, b], c  A4: c, a,
and R4 = A1: [a, b], [c, d]  A2: [a, d], [b, c]  A3: c, [a, b], d  A4: a, d,
and R5 = A1: [c, d], [a, b]  A2: [a, b], [c, d]  A3: [a, c], d, b  A4: d, [a, b], c,
and R6 = A1: [a, b], [c, d]  A2: [c, d], [a, b]  A3: [a, c], [b, d]  A4: d, b,
and R7 = A1: [a, b], [c, d]  A2: [c, d], [a, b]  A3: a, c, d, b  A4: d, [a, b], c,
and R8 = A1: [a, b], [c, d]  A2: [a, c], [b, d]  A3: d, [a, b], c  A4: d, c,
and R9 = A1: [a, b], [c, d]  A2: [a, d], [c, b]  A3: d, c, [a, b]  A4: [a, b], c,
and R10 = A1: [a, b], [c, d]  A2: [c, d], [a, b]  A3: [a, c], d, b  A4: [b, d], a, c,
and R11 = A1: [a, b], [c, d]  A2: [c, d], [a, b]  A3: d, [a, b], c  A4: c, a,
and R12 = A1: [c, d], [a, b]  A2: [a, b], [c, d]  A3: a, [c, d], b  A4: c, b,
and R13 = A1: [a, c], [b, d]  A2: [c, d], a, b  A3: [b, d], a, c  A4: a, b,
and R14 = A1: [a, b], [c, d]  A2: d, c, [a, b]  A3: [a, b], c, d  A4: a, d,
and R15 = A1: [a, b], [c, d]  A2: [c, d], [a, b]  A3: [b, d], a, c  A4: a, c,
\[
\begin{align*}
\text{and} & \quad R16 = A1: [a, b], [c, d] & A2: [c, d], [a, b] & A3: a, c, d, b & A4: [a, b, d], c \\
\text{and} & \quad R17 = A1: [a, b], [c, d] & A2: [c, d], [a, b] & A3: [a, c], [b, d] & A4: d, [a, b] \\
\text{and} & \quad R18 = A1: [a, b], [c, d] & A2: [a, d], [b, c] & A3: [a, b, c], d & A4: d, c, [a, b] \\
\text{and} & \quad R19 = A1: [a, b], [c, d] & A2: [c, d], [a, b] & A3: [b, d], a, c & A4: [a, b, d] \\
\text{and} & \quad R20 = A1: [b, a], [c, d] & A2: b, a, [c, d] & A3: a, c, [b, d] & A4: d, c, [a, b] \\
\text{and} & \quad R21 = A1: [a, d], c, b & A2: d, c, [a, b] & A3: c, [a, b], d & A4: a, b, [c, d] \\
\text{and} & \quad R22 = A1: [a, c], d, b & A2: d, c, [a, b] & A3: d, [a, b], c & A4: a, b, [c, d] \\
\text{and} & \quad R23 = A1: [a, b], [c, d] & A2: [c, d], [a, b] & A3: [a, c], [b, d] & A4: [a, b, d] \\
\text{and} & \quad R24 = A1: [c, d], [a, b] & A2: d, b, a, c & A3: c, a, [b, d] & A4: b, a, [c, d] \\
\text{and} & \quad R25 = A1: [c, d], [a, b] & A2: [b, d], a, c & A3: a, b, [c, d] & A4: a, c, [b, d] \\
\text{and} & \quad R26 = A1: [b, a], [c, d] & A2: [c, d], [a, b] & A3: a, b, [c, d] & A4: a, c, [b, d] \\
\text{and} & \quad R27 = A1: [a, b], [c, d] & A2: [b, d], a, c & A3: [a, c], [b, d] & A4: [c, d], a, b \\
\text{and} & \quad R28 = A1: [c, d], a, b & A2: [b, d], a, c & A3: a, b, [c, d] & A4: a, c, [b, d] \\
\text{and} & \quad R29 = A1: [a, c], d, b & A2: [b, d], a, c & A3: a, b, [c, d] & A4: a, d, [c, b] \\
\text{and} & \quad R30 = A1: [a, c], d, b & A2: d, c, [a, b] & A3: c, [a, b], d & A4: [a, b, d] \\
\text{and} & \quad R31 = A1: [b, d], a, c & A2: [a, c], d, b & A3: c, d, [a, b] & A4: [a, b, c] \\
\text{and} & \quad R32 = A1: [a, c], d, b & A2: d, c, [a, b] & A3: d, [a, b], c & A4: [a, b, c] \\
\text{and} & \quad R33 = A1: [c, d], [a, b] & A2: [a, c], d, b & A3: a, b, [c, d] & A4: d, [a, b] \\
\text{and} & \quad R34 = A1: [a, b], [c, d] & A2: a, c, d, b & A3: b, [a, d], c & A4: c, d, [a, b] \\
\text{and} & \quad R35 = A1: [a, c], d, b & A2: a, [a, b], c, d & A3: a, b, [c, d] & A4: d, c, [a, b] \\
\text{and} & \quad R36 = A1: [c, d], [a, b] & A2: [a, c], d, b & A3: [b, d], a, c & A4: a, b, [c, d] \\
\text{and} & \quad R37 = A1: [a, c], [b, d] & A2: [b, d], [a, c] & A3: a, b, [c, d] & A4: c, d, [a, b] \\
\text{and} & \quad R38 = A1: [c, d], a, b & A2: [b, d], a, c & A3: a, b, [c, d] & A4: [a, b, d] \\
\text{and} & \quad R39 = A1: [a, c], d, b & A2: [b, d], a, c & A3: a, b, [c, d] & A4: [c, d], a, b \\
\text{and} & \quad R40 = A1: [a, d], c, b & A2: [a, b], c, d & A3: [a, b, c], d & A4: d, c, [a, b] \\
\end{align*}
\]
derive-orbit-equations (an-sds)
R10 R26 R27 R28 R29 R43 R45
by simp-all

prove-inefficient-supports (ex-post-efficient-sds sd-efficient-sds)
R3 [b] and R4 [b] and R5 [b] and R7 [b] and R8 [b] and
R9 [b] and R11 [b] and R12 [b] and R14 [b] and R16 [b] and
R17 [b] and R18 [b] and R21 [b] and R22 [b] and R23 [b] and
R30 [b] and R32 [b] and R33 [b] and R35 [b] and R40 [b] and
R41 [b] and R43 [b] and R44 [b] and R47 [b] and
R10 [c, b] witness: [a: 1 / 2, b: 0, c: 0, d: 1 / 2] and
R15 [c, b] witness: [a: 1 / 2, b: 0, c: 0, d: 1 / 2] and
R19 [c, b] witness: [a: 1 / 2, b: 0, c: 0, d: 1 / 2] and
R25 [b, c] witness: [c: 0, d: 1 / 2, a: 1 / 2, b: 0] and
R26 [c, b] witness: [b: 0, d: 1 / 2, a: 1 / 2, c: 0] and
R27 [c, b] witness: [a: 1 / 2, b: 0, c: 0, d: 1 / 2] and
R28 [b, c] witness: [c: 0, d: 1 / 2, a: 1 / 2, b: 0] and
R29 [b, c] witness: [a: 1 / 2, c: 0, d: 1 / 2, b: 0] and
R39 [b, c] witness: [a: 1 / 2, c: 0, d: 1 / 2, b: 0]
by (simp-all add: agent-iff alt-iff)

derive-strategyproofness-conditions (strategyproof-an-sds)
distance: 2
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 R11 R12 R13 R14 R15 R16 R17 R18 R19 R20
R41 R42 R43 R44 R45 R46 R47
by (simp-all add: agent-iff alt-iff)

lemma lottery-conditions:
assumes is-pref-profile R
shows  \( \text{pmf (sds R)} \ a \geq 0 \ \text{pmf (sds R)} \ b \geq 0 \ \text{pmf (sds R)} \ c \geq 0 \ \text{pmf (sds R)} \ d \geq 0 \)
\( \text{pmf (sds R)} \ a + \text{pmf (sds R)} \ b + \text{pmf (sds R)} \ c + \text{pmf (sds R)} \ d = 1 \)
using lottery-prob-alls[OF sds-wf[OF assms]]
by (simp-all add: alts pmf-nonneg measure-measure-pmf-finite)

1.3 Main Proof

lemma R45 [simp]: \( \text{pmf (sds R45)} \ a = \frac{1}{4} \ \text{pmf (sds R45)} \ b = \frac{1}{4} \ \text{pmf (sds R45)} \ c = \frac{1}{4} \ \text{pmf (sds R45)} \ d = \frac{1}{4} \)
using R45.orbits lottery-conditions[OF R45.wf] by simp-all

lemma R10-bc [simp]: \( \text{pmf (sds R10)} \ b = 0 \ \text{pmf (sds R10)} \ c = 0 \)
using R10-support R10.orbits by auto

lemma R10-ad [simp]: \( \text{pmf (sds R10)} \ a = \frac{1}{2} \ \text{pmf (sds R10)} \ d = \frac{1}{2} \)
using lottery-conditions[OF R10.wf R10-bc R10.orbits] by simp-all

lemma R26-bc [simp]: \( \text{pmf (sds R26)} \ b = 0 \ \text{pmf (sds R26)} \ c = 0 \)
using R26-support R26.orbits by auto

lemma R26-d [simp]: \( \text{pmf (sds R26)} \ d = 1 - \text{pmf (sds R26)} \ a \)
using lottery-conditions[OF R26.wf R26-bc] R26-orbits by simp

lemma R27-bc [simp]: \( \text{pmf (sds R27)} \ b = 0 \ \text{pmf (sds R27)} \ c = 0 \)
using R27-support R27.orbits by auto

lemma R27-d [simp]: \( \text{pmf (sds R27)} \ d = 1 - \text{pmf (sds R27)} \ a \)
using lottery-conditions[OF R27.wf R27-bc] R27-orbits by simp

lemma R28-bc [simp]: \( \text{pmf (sds R28)} \ b = 0 \ \text{pmf (sds R28)} \ c = 0 \)
using R28-support R28.orbits by auto

lemma R28-d [simp]: \( \text{pmf (sds R28)} \ d = 1 - \text{pmf (sds R28)} \ a \)
using lottery-conditions[OF R28.wf R28-bc] R28-orbits by simp

lemma R29-bc [simp]: \( \text{pmf (sds R29)} \ b = 0 \ \text{pmf (sds R29)} \ c = 0 \)
using R29-support R29.orbits by auto

lemma R29-ac [simp]: \( \text{pmf (sds R29)} \ a = \frac{1}{2} \ \text{pmf (sds R29)} \ d = \frac{1}{2} \)
using lottery-conditions[OF R29.wf R29-bc R29.orbits] R29-ac by simp-all

lemmas R43-bc [simp] = R43-support
lemma R43-ad [simp]: pmf (sds R43) a = 1/2 pmf (sds R43) d = 1/2
using lottery-conditions[OF R43_wf] R43-bc R43.orbits by simp-all

lemma R39-b [simp]: pmf (sds R39) b = 0
proof –
  { 
    assume [simp]: pmf (sds R39) c = 0
    with R29-R39.strategyproofness(1)
    have pmf (sds R39) d ≤ 1/2 by auto
    with R39-R29.strategyproofness(1) lottery-conditions[OF R39_wf]
    have pmf (sds R39) b = 0 by auto
  }
  with R39.support show ?thesis by blast
qed

lemma R36-a [simp]: pmf (sds R36) a = 1/2 and R36-b [simp]: pmf (sds R36) b = 0
proof –
  from R10-R36.strategyproofness(1) lottery-conditions[OF R36_wf]
  have pmf (sds R36) a + pmf (sds R36) b ≤ 1/2 by auto
  with R36-R10.strategyproofness(1) lottery-conditions[OF R36_wf]
  show pmf (sds R36) a = 1/2 pmf (sds R36) b = 0 by auto
qed

lemma R39-a [simp]: pmf (sds R39) a = 1/2
proof –
  from R36-R39.strategyproofness(1) lottery-conditions[OF R39_wf]
  have pmf (sds R39) a ≥ 1/2 by auto
  with R39-R36.strategyproofness(1) lottery-conditions[OF R39_wf]
  show ?thesis by auto
qed

lemma R39-d [simp]: pmf (sds R39) d = 1/2 - pmf (sds R39) c
using lottery-conditions[OF R39_wf] by simp

lemmas R12-b [simp] = R12.support

lemma R12-c [simp]: pmf (sds R12) c = 0
using R12-R10.strategyproofness(1) lottery-conditions[OF R12_wf]
by (auto simp del: pmf-nonneg)

lemma R12-d [simp]: pmf (sds R12) d = 1 - pmf (sds R12) a
using lottery-conditions[OF R12 wf] by simp

lemma R12-a-ge-one-half: pmf (sds R12) a ≥ 1/2
  using R10-R12.strategyproofness(1) lottery-conditions[OF R12 wf]
  by auto

lemma R44 [simp]:
  pmf (sds R44) a = pmf (sds R12) a pmf (sds R44) d = 1 - pmf (sds R12) a
  pmf (sds R44) b = 0 pmf (sds R44) c = 0
proof –
  from R12-R44.strategyproofness(1) R44.support have pmf (sds R44) a ≤ pmf (sds R12) a
    by simp
with R44-R12.strategyproofness(1) R44.support lottery-conditions[OF R44 wf]
  show pmf (sds R44) a = pmf (sds R12) a pmf (sds R44) c = 0
  pmf (sds R44) d = 1 - pmf (sds R12) a
qed (insert R44.support, simp-all)

lemma R9-a [simp]: pmf (sds R9) a = pmf (sds R35) a
proof –
  from R9-R35.strategyproofness(1) R35.support R9.support
    have pmf (sds R35) a ≤ pmf (sds R9) a
      by simp
with R35-R9.strategyproofness(1) R9.support R35.support
  show ?thesis by simp
qed

lemma R18-c [simp]: pmf (sds R18) c = pmf (sds R9) c
proof –
  from R18-R9.strategyproofness(1) R18.support R9.support
    have pmf (sds R18) d + pmf (sds R18) a ≥ pmf (sds R9) d + pmf (sds R9)
      a
      by auto
with R9-R18.strategyproofness(1) R18.support R9.support
  lottery-conditions[OF R9 wf] lottery-conditions[OF R18 wf]
  show ?thesis by auto
qed

lemma R5-d-ge-one-half: pmf (sds R5) d ≥ 1/2
  using R5-R10.strategyproofness(1) R5.support lottery-conditions[OF R5 wf]
  by auto

lemma R7 [simp]: pmf (sds R7) a = 1/2 pmf (sds R7) b = 0 pmf (sds R7) c = 0
  pmf (sds R7) d = 1/2
proof –
  from R5-d-ge-one-half have 1/2 ≤ pmf (sds R5) d
    by simp
  also from R5-R17.strategyproofness(1) R17.support lottery-conditions[OF R5 wf]
  lottery-conditions[OF R17 wf]
    have . . . ≤ pmf (sds R17) d
    by (auto simp del: pmf-nonneg)
  also from R17-R7.strategyproofness(1) lottery-conditions[OF R7 wf]
  lottery-conditions[OF R17 wf] R7.support
have \( \text{pmf} \ (sds \ R17) \ d \leq \text{pmf} \ (sds \ R7) \ d \) by (auto simp del: pmf-nonneg)
finally have \( \text{pmf} \ (sds \ R7) \ d \geq 1/2 \).
with \( R7-R13.\text{strategyproofness}(1) \) lottery-conditions[OF R7.wf] R7.support
  show \( \text{pmf} \ (sds \ R7) \ a = 1/2 \) \( \text{pmf} \ (sds \ R7) \ b = 0 \) \( \text{pmf} \ (sds \ R7) \ c = 0 \) \( \text{pmf} \ (sds \ R7) \ d = 1/2 \)
  by auto
qed

lemma R5 [simp]: \( \text{pmf} \ (sds \ R5) \ a = 1/2 \) \( \text{pmf} \ (sds \ R5) \ b = 0 \) \( \text{pmf} \ (sds \ R5) \ c = 0 \) \( \text{pmf} \ (sds \ R5) \ d = 1/2 \)
proof –
  from R5-R7.\text{strategyproofness}(1) lottery-conditions[OF R5.wf] R5.support
  have \( \text{pmf} \ (sds \ R5) \ d \leq 1/2 \) by auto
with \( R5-d-ge-one-half \) show \( \text{pmf} \ (sds \ R5) \ d = 1/2 \) by simp
with \( R5-R10.\text{strategyproofness}(1) \) lottery-conditions[OF R5.wf] R5.support
  show \( \text{pmf} \ (sds \ R5) \ c = 0 \) \( \text{pmf} \ (sds \ R5) \ a = 1/2 \) by simp-all
qed (simp-all add: R5.support)

lemma R15 [simp]: \( \text{pmf} \ (sds \ R15) \ a = 1/2 \) \( \text{pmf} \ (sds \ R15) \ b = 0 \) \( \text{pmf} \ (sds \ R15) \ c = 0 \) \( \text{pmf} \ (sds \ R15) \ d = 1/2 \)
proof –
  { 
    assume \( \text{pmf} \ (sds \ R15) \ b = 0 \)
    with \( R10-R15.\text{strategyproofness}(1) \) lottery-conditions[OF R15.wf]
      have \( \text{pmf} \ (sds \ R15) \ a + \text{pmf} \ (sds \ R15) \ c \leq 1/2 \) by auto
    with \( R15-R10.\text{strategyproofness}(1) \) lottery-conditions[OF R15.wf]
      have \( \text{pmf} \ (sds \ R15) \ c = 0 \) by auto
  }
with \( R15.\text{support} \) show [simp]: \( \text{pmf} \ (sds \ R15) \ c = 0 \) by blast
with \( R15-R5.\text{strategyproofness}(1) \) lottery-conditions[OF R15.wf]
  have \( \text{pmf} \ (sds \ R15) \ a \geq 1/2 \) by auto
moreover from \( R15-R7.\text{strategyproofness}(1) \) lottery-conditions[OF R15.wf]
  have \( \text{pmf} \ (sds \ R15) \ b + \text{pmf} \ (sds \ R15) \ d \geq 1/2 \) by auto
ultimately show \( \text{pmf} \ (sds \ R15) \ a = 1/2 \) using lottery-conditions[OF R15.wf]
by auto
with \( R15-R5.\text{strategyproofness}(1) \) lottery-conditions[OF R15.wf]
  show \( \text{pmf} \ (sds \ R15) \ d = 1/2 \) \( \text{pmf} \ (sds \ R15) \ b = 0 \) by auto
qed

lemma R13-aux: \( \text{pmf} \ (sds \ R13) \ b = 0 \) \( \text{pmf} \ (sds \ R13) \ c = 0 \) \( \text{pmf} \ (sds \ R13) \ d = 1 - \text{pmf} \ (sds \ R13) \ a \)
  and \( R27-R13.\text{simp} \): \( \text{pmf} \ (sds \ R27) \ a = \text{pmf} \ (sds \ R13) \ a \)
using \( R27-R13.\text{strategyproofness}(1) R13-R27.\text{strategyproofness}(1) \) lottery-conditions[OF R13.wf] by auto

lemma R13 [simp]: \( \text{pmf} \ (sds \ R13) \ a = 1/2 \) \( \text{pmf} \ (sds \ R13) \ b = 0 \) \( \text{pmf} \ (sds \ R13) \ c = 0 \) \( \text{pmf} \ (sds \ R13) \ d = 1/2 \)
  using \( R13-R13.\text{strategyproofness}(1) \) \( R13-R15.\text{strategyproofness}(1) \) \( R13-aux \) by simp-all
**lemma** \( R27 \) \([\text{smp}]\): \( \text{pmf} \ (sds \ R27) \ a = 1/2 \ \text{pmf} \ (sds \ R27) \ b = 0 \ \text{pmf} \ (sds \ R27) \ c = 0 \ \text{pmf} \ (sds \ R27) \ d = 1/2 \)

by \( \text{smp-all} \)

**lemma** \( R19 \) \([\text{smp}]\): \( \text{pmf} \ (sds \ R19) \ a = 1/2 \ \land \ \text{pmf} \ (sds \ R19) \ b = 0 \ \land \ \text{pmf} \ (sds \ R19) \ c = 0 \ \land \ \text{pmf} \ (sds \ R19) \ d = 1/2 \)

**proof** –

\[\text{have} \ \text{pmf} \ (sds \ R19) \ a = 1/2 \ \land \ \text{pmf} \ (sds \ R19) \ b = 0 \ \land \ \text{pmf} \ (sds \ R19) \ c = 0 \ \land \ \text{pmf} \ (sds \ R19) \ d = 1/2 \]

**proof** \( \text{rule} \ \text{disj[OF} \ R19.\text{support}\]; \ \text{safe} \)

assume \([\text{smp}]\): \( \text{pmf} \ (sds \ R19) \ b = 0 \)

from \( \text{R10-R19.strategyproofness(1)} \ \text{lottery-conditions}[\text{OF} \ R19.\text{wf}] \)

have \( \text{pmf} \ (sds \ R19) \ a + \ \text{pmf} \ (sds \ R19) \ c \leq 1/2 \) by \( \text{auto} \)

moreover from \( \text{R19-R10.strategyproofness(1)} \)

have \( \text{pmf} \ (sds \ R19) \ a + \ \text{pmf} \ (sds \ R19) \ c \geq 1/2 \) by \( \text{simp} \)

ultimately show \( \text{pmf} \ (sds \ R19) \ d = 1/2 \) using \( \text{lottery-conditions}[\text{OF} \ R19.\text{wf}] \)

by \( \text{smp} \)

with \( \text{R27-R19.strategyproofness(1)} \ \text{lottery-conditions}[\text{OF} \ R19.\text{wf}] \)

show \( \text{pmf} \ (sds \ R19) \ a = 1/2 \ \text{pmf} \ (sds \ R19) \ c = 0 \) by \( \text{auto} \)

next

assume \([\text{smp}]\): \( \text{pmf} \ (sds \ R19) \ c = 0 \)

from \( \text{R19-R10.strategyproofness(1)} \ \text{have} \ \text{pmf} \ (sds \ R19) \ a \geq 1/2 \) by \( \text{auto} \)

moreover from \( \text{R19-R27.strategyproofproofness(1)} \ \text{have} \ \text{pmf} \ (sds \ R19) \ d \geq 1/2 \)

by \( \text{auto} \)

ultimately show \( \text{pmf} \ (sds \ R19) \ a = 1/2 \ \text{pmf} \ (sds \ R19) \ d = 1/2 \) \( \text{pmf} \ (sds \ R19) \ b = 0 \)

using \( \text{lottery-conditions}[\text{OF} \ R19.\text{wf}] \) by \( \text{auto simp del: pmf-nonneg} \)

qed

thus \( \text{pmf} \ (sds \ R19) \ a = 1/2 \ \text{pmf} \ (sds \ R19) \ b = 0 \ \text{pmf} \ (sds \ R19) \ c = 0 \ \text{pmf} \ (sds \ R19) \ d = 1/2 \)

by \( \text{blast+} \)

qed

**lemma** \( R1 \) \([\text{smp}]\): \( \text{pmf} \ (sds \ R1) \ a = 1/2 \ \text{pmf} \ (sds \ R1) \ b = 0 \)

**proof** –

from \( \text{R19-R1.strategyproofproofness(1)} \ \text{lottery-conditions}[\text{OF} \ R1.\text{wf}] \)

have \( \text{pmf} \ (sds \ R1) \ a + \ \text{pmf} \ (sds \ R1) \ b \leq 1/2 \) by \( \text{simp} \)

with \( \text{R1-R19.strategyproofproofness(1)} \ \text{lottery-conditions}[\text{OF} \ R1.\text{wf}] \)

show \( \text{pmf} \ (sds \ R1) \ a = 1/2 \ \text{pmf} \ (sds \ R1) \ b = 0 \) by \( \text{auto} \)

qed

**lemma** \( R22 \) \([\text{smp}]\): \( \text{pmf} \ (sds \ R22) \ a = 1/2 \ \text{pmf} \ (sds \ R22) \ b = 0 \ \text{pmf} \ (sds \ R22) \ c = 0 \ \text{pmf} \ (sds \ R22) \ d = 1/2 \)

**proof** –

from \( \text{R33-R5.strategyproofproofness(1)} \ \text{R33.support} \)

have \( 1/2 \leq \ \text{pmf} \ (sds \ R33) \) by \( \text{auto} \)

also from \( \text{R33-R22.strategyproofproofness(1)} \ \text{R22.support} \ \text{R33.support} \ \text{lottery-conditions}[\text{OF} \ R22.\text{wf}] \ \text{lottery-conditions}[\text{OF} \ R33.\text{wf}] \)
have \( \cdots \leq \text{pmf} (sds R22) a \) by simp

finally show \( \text{pmf} (sds R22) a = 1/2 \) pmf \( (sds R22) b = 0 \) pmf \( (sds R22) c = 0 \) pmf \( (sds R22) d = 1/2 \)

using \( R22-R29.\text{strategyproofness}(1) \) lottery-conditions[\( OF \ R22.\text{wf} \)] by (auto simp del: pmf-nonneg)

qed

lemma \( R28 \) [simp]; pmf \( (sds R28) a = 1/2 \) pmf \( (sds R28) b = 0 \) pmf \( (sds R28) c = 0 \) pmf \( (sds R28) d = 1/2 \)

proof –

have pmf \( (sds R28) a \leq \text{pmf} (sds R32) d \)

using \( R32-R28.\text{strategyproofness}(1) \) lottery-conditions[\( OF \ R32.\text{wf} \)] by auto

hence \( R32-d: \text{pmf} (sds R32) d = \text{pmf} (sds R28) a \)

using \( R28-R32.\text{strategyproofness}(1) \) lottery-conditions[\( OF \ R32.\text{wf} \)] by auto

from \( R22-R32.\text{strategyproofness}(1) \) lottery-conditions[\( OF \ R32.\text{wf} \)] \( R32.\text{support} \)

have pmf \( (sds R32) a \leq 1/2 \) by auto

with \( R32-R22.\text{strategyproofness}(1) \) lottery-conditions[\( OF \ R32.\text{wf} \)] \( R32.\text{support} \)

show pmf \( (sds R28) a = 1/2 \) pmf \( (sds R28) b = 0 \) pmf \( (sds R28) c = 0 \) pmf \( (sds R28) d = 1/2 \)

by (auto simp: \( R32-d \) simp del: pmf-nonneg)

qed

lemma \( R39 \) [simp]; pmf \( (sds R39) a = 1/2 \) pmf \( (sds R39) b = 0 \) pmf \( (sds R39) c = 0 \) pmf \( (sds R39) d = 1/2 \)

proof –

from \( R28-R39.\text{strategyproofness}(1) \) show pmf \( (sds R39) c = 0 \) by simp

thus pmf \( (sds R39) a = 1/2 \) pmf \( (sds R39) b = 0 \) pmf \( (sds R39) d = 1/2 \)

by simp-all

qed

lemma \( R2 \) [simp]; pmf \( (sds R2) a = 1/2 \) pmf \( (sds R2) b = 0 \) pmf \( (sds R2) c = 0 \) pmf \( (sds R2) d = 1/2 \)

proof –

from \( R1-R2.\text{strategyproofness}(1) \) \( R2-R1.\text{strategyproofness}(1) \) lottery-conditions[\( OF \ R2.\text{wf} \)] lottery-conditions[\( OF \ R1.\text{wf} \)]

have pmf \( (sds R2) a = 1/2 \) pmf \( (sds R2) c + \text{pmf} (sds R2) d = 1/2 \)

by (auto simp: \text{algebra-simps simp del: pmf-nonneg})

with \( R39-R2.\text{strategyproofness}(1) \) lottery-conditions[\( OF \ R2.\text{wf} \)]

show pmf \( (sds R2) a = 1/2 \) pmf \( (sds R2) b = 0 \) pmf \( (sds R2) c = 0 \) pmf \( (sds R2) d = 1/2 \)

by auto

qed

lemma \( R42 \) [simp]; pmf \( (sds R42) a = 0 \) pmf \( (sds R42) b = 0 \) pmf \( (sds R42) c = 1/2 \) pmf \( (sds R42) d = 1/2 \)

proof –

from \( R17-R5.\text{strategyproofness}(1) \) lottery-conditions[\( OF \ R17.\text{wf} \)] \( R17.\text{support} \)

have pmf \( (sds R17) d \leq 1/2 \) by auto
moreover from \(R5-R17\).strategyproofness(1) \(R17\).support lottery-conditions\(\lfloor\) \(OF R17\.wf\)\]
   have \(pmf (sds R17, d \geq 1/2)\) by auto
ultimately have \(R17\_d\_pmf (sds R17, d = 1/2)\) by simp

from \(R6-R42\).strategyproofness(1)
   have \(pmf (sds R42, a + pmf (sds R42) c \leq pmf (sds R6, a + pmf (sds R6) c)\) by simp
also from \(R6-R19\).strategyproofness(1) \(\mathit{lottery-conditions}[OF R6\_wf]\)
   have \(pmf (sds R6, a + pmf (sds R6) c \leq 1/2)\) by (auto simp del: pmf-nonneg)
finally have \(pmf (sds R42, a + pmf (sds R42) c \leq 1/2)\).
moreover from \(R17-R11\).strategyproofness(1) \(R11\_support R17\_support \mathit{lottery-conditions}[OF R11\_wf]\) \(\mathit{lottery-conditions}[OF R17\_wf]\)
   have \(pmf (sds R11, d \geq 1/2)\) by (auto simp: R17-d)
ultimately have \(pmf (sds R42, a + pmf (sds R42) c \leq pmf (sds R11, d)\) by simp
with \(R42-R11\).strategyproofness(1) \(R11\_support \mathit{pmf (sds R11, d \leq pmf (sds R42) c}\) by auto
with \(\mathit{\phi pmf (sds R11, d \geq 1/2) have pmf (sds R42) c \geq 1/2}\) by simp
moreover from \(R17-R3\).strategyproofness(1) \(R3\_support R17\_support \mathit{pmf (sds R3, d \geq 1/2}\) by (auto simp: R17-d)
ultimately show \(pmf (sds R42, a = 0 pmf (sds R42) b = 0 pmf (sds R42) c = 1/2 pmf (sds R42) d = 1/2)\)
   using \(R42-R3\).strategyproofness(1) \(\mathit{lottery-conditions}[OF R3\_wf]\) \(\mathit{lottery-conditions}[OF R42\_wf]\)
   by linarith+
qed

lemma \(R37\_simp\): \(pmf (sds R37, a = 1/2 pmf (sds R37) b = 0 pmf (sds R37) c = 1/2 pmf (sds R37) d = 0)\)
proof –
   from \(R37-R42\).strategyproofness(1) \(\mathit{lottery-conditions}[OF R37\_wf]\)
   have \(pmf (sds R37, a = 1/2 \lor pmf (sds R37) a + pmf (sds R37) b \geq 1/2)\)
   by (auto simp del: pmf-nonneg)
moreover from \(R37-R42\).strategyproofness(2) \(\mathit{lottery-conditions}[OF R37\_wf]\)
   have \(pmf (sds R37, c = 1/2 \lor pmf (sds R37) c + pmf (sds R37) d \geq 1/2)\)
   by (auto simp del: pmf-nonneg)
ultimately show \(pmf (sds R37, a = 1/2 pmf (sds R37) b = 0 pmf (sds R37) c = 1/2 pmf (sds R37) d = 0)\)
   using \(\mathit{lottery-conditions}[OF R37\_wf]\) by (auto simp del: pmf-nonneg)
qed

lemma \(R24\_simp\): \(pmf (sds R24, a = 0 pmf (sds R24) b = 0 pmf (sds R24) d = 1 - pmf (sds R24) c\)
   using \(R42-R24\).strategyproofness(1) \(\mathit{lottery-conditions}[OF R24\_wf]\) by (auto simp del: pmf-nonneg)

lemma \(R34\_simp\):
\[
\text{proof} - \\
\text{from } R_{24-R34}.\text{strategyproofness}(1) \text{ lottery-conditions[OF R34.wf]}
\hspace{1em} \text{have } \text{pmf } (\text{sds R34}) \ b \leq \text{pmf } (\text{sds R24}) \ c \ \text{by (auto simp del: pmf-nonneg)}
\hspace{1em} \text{moreover from } R_{34-R24}.\text{strategyproofness}(1) \text{ lottery-conditions[OF R34.wf]}
\hspace{1em} \text{have } \text{pmf } (\text{sds R34}) \ b \geq \text{pmf } (\text{sds R24}) \ c \ \text{by auto}
\hspace{1em} \text{ultimately show } bc: \text{pmf } (\text{sds R34}) \ b = \text{pmf } (\text{sds R24}) \ c \ \text{by simp}
\hspace{1em} \text{from } R_{34-R24}.\text{strategyproofness}(1) \text{ bc lottery-conditions[OF R34.wf]}
\hspace{1em} \text{show } \text{pmf } (\text{sds R34}) \ c = 0 \ \text{by auto}
\hspace{1em} \text{moreover from } R_{24-R34}.\text{strategyproofness}(1) \text{ be show } \text{pmf } (\text{sds R34}) \ d = 0
\hspace{1em} \text{by simp}
\hspace{1em} \text{ultimately show } \text{pmf } (\text{sds R34}) \ a = 1 - \text{pmf } (\text{sds R24}) \ c
\hspace{1em} \text{using } bc \text{ lottery-conditions[OF R34.wf] by auto}
\hspace{1em} \text{qed}
\]

\text{lemma } R_{14} \text{ [simp]; } \text{pmf } (\text{sds R14}) \ b = 0 \ \text{pmf } (\text{sds R14}) \ d = 0 \ \text{pmf } (\text{sds R14}) \ c
\hspace{1em} \text{by (auto simp del: pmf-nonneg)}

\text{lemma } R_{46} \text{ [simp]; } \text{pmf } (\text{sds R46}) \ a = 0 \ \text{pmf } (\text{sds R46}) \ c = 0 \ \text{pmf } (\text{sds R46}) \ d
\hspace{1em} \text{by (auto simp del: pmf-nonneg)}

\text{lemma } R_{20} \text{ [simp]; } \text{pmf } (\text{sds R20}) \ a = 0 \ \text{pmf } (\text{sds R20}) \ c = 0 \ \text{pmf } (\text{sds R20}) \ d
\hspace{1em} \text{by (auto simp del: pmf-nonneg)}

\text{lemma } R_{21} \text{ [simp]; } \text{pmf } (\text{sds R21}) \ d = 1 - \text{pmf } (\text{sds R21}) \ a \ \text{pmf } (\text{sds R21}) \ b
\hspace{1em} \text{by (auto simp del: pmf-nonneg)}

\text{lemma } R_{16-R12}: \text{pmf } (\text{sds R16}) \ c + \text{pmf } (\text{sds R16}) \ a \leq \text{pmf } (\text{sds R12}) \ a
\hspace{1em} \text{by auto}

\text{lemma } R_{16} \text{ [simp]; } \text{pmf } (\text{sds R16}) \ b = 0 \ \text{pmf } (\text{sds R16}) \ c = 0 \ \text{pmf } (\text{sds R16}) \ d
\hspace{1em} \text{by auto}

\text{proof} - \\
\hspace{1em} \text{from } R_{16-R12} \text{ have } \text{pmf } (\text{sds R16}) \ c + \text{pmf } (\text{sds R16}) \ a \leq \text{pmf } (\text{sds R12}) \ a
\hspace{1em} \text{by simp}
\hspace{1em} \text{also from } R_{44-R40}.\text{strategyproofness}(1) \text{ lottery-conditions[OF R40.wf] R40.support}
\hspace{1em} \text{have } \text{pmf } (\text{sds R12}) \ a \leq \text{pmf } (\text{sds R40}) \ a \ \text{by auto}
\hspace{1em} \text{also from } R_{9-R40}.\text{strategyproofness}(1) \text{ R9.support R40.support}
\hspace{1em} \text{have } \text{pmf } (\text{sds R40}) \ a \leq \text{pmf } (\text{sds R9}) \ a \ \text{by auto}
finally have \( \text{pmf} \ (\text{sds R16}) \ c + \text{pmf} \ (\text{sds R16}) \ a \leq \text{pmf} \ (\text{sds R9}) \ a \) by simp

moreover from \( R14\text{-}R16.\text{strategyproofness}(1) \) \( \text{R16.\text{support \ lottery-conditions}}[\text{OF R16.wf}] \)

have \( \text{pmf} \ (\text{sds R16}) \ a \geq \text{pmf} \ (\text{sds R14}) \ a \) by auto

ultimately have \( \text{pmf} \ (\text{sds R16}) \ c \leq \text{pmf} \ (\text{sds R9}) \ a - \text{pmf} \ (\text{sds R14}) \ a \) by simp

also from \( R14\text{-}R9.\text{strategyproofness}(1) \) \( \text{R9.\text{support \ lottery-conditions}}[\text{OF R9.wf}] \)

have \( \text{pmf} \ (\text{sds R9}) \ a - \text{pmf} \ (\text{sds R14}) \ a \leq 0 \) by (auto simp del: pmf-nonneg)

finally show \( \text{pmf} \ (\text{sds R16}) \ b = 0 \) \( \text{pmf} \ (\text{sds R16}) \ c = 0 \) \( \text{pmf} \ (\text{sds R16}) \ d = 1 - \text{pmf} \ (\text{sds R16}) \ a \)

using lottery-conditions[\text{OF R16.wf}] \( \text{R16.\text{support}} \) by auto

qed

lemma \( R12\text{-}R14 \): \( \text{pmf} \ (\text{sds R14}) \ a \leq \text{pmf} \ (\text{sds R12}) \ a \)

using \( R14\text{-}R16.\text{strategyproofness}(1) \) \( \text{R16\text{-}R12} \) by auto

lemma \( R12\text{-}a \) [simp]: \( \text{pmf} \ (\text{sds R12}) \ a = \text{pmf} \ (\text{sds R9}) \ a \)

proof –

from \( R44\text{-}R40.\text{strategyproofness}(1) \) \( \text{R40.\text{support \ lottery-conditions}}[\text{OF R40.wf}] \)

have \( \text{pmf} \ (\text{sds R12}) \ a \leq \text{pmf} \ (\text{sds R40}) \ a \) by auto

also from \( R9\text{-}R40.\text{strategyproofness}(1) \) \( \text{R40.\text{support}} \)

have \( \text{pmf} \ (\text{sds R40}) \ a \leq \text{pmf} \ (\text{sds R9}) \ a \) by auto

finally have \( B \): \( \text{pmf} \ (\text{sds R12}) \ a \leq \text{pmf} \ (\text{sds R9}) \ a \) by simp

moreover from \( R14\text{-}R9.\text{strategyproofness}(1) \) \( \text{R9.\text{support \ lottery-conditions}}[\text{OF R9.wf}] \) \( \text{R9.\text{support}} \)

have \( \text{pmf} \ (\text{sds R9}) \ a \leq \text{pmf} \ (\text{sds R14}) \ a \) by (auto simp del: pmf-nonneg)

with \( R12\text{-}R14 \) have \( \text{pmf} \ (\text{sds R9}) \ a \leq \text{pmf} \ (\text{sds R12}) \ a \) by simp

ultimately show \( \text{pmf} \ (\text{sds R12}) \ a = \text{pmf} \ (\text{sds R9}) \ a \) by simp

qed

lemma \( R9 \) [simp]: \( \text{pmf} \ (\text{sds R9}) \ b = 0 \) \( \text{pmf} \ (\text{sds R9}) \ d = 0 \)

pmf \ (\text{sds R14}) \ a = pmf \ (\text{sds R35}) \ a \ pmf \ (\text{sds R9}) \ c = 1 - \ pmf \ (\text{sds R35}) \ a

using \( R12\text{-}R14 \) \( R14\text{-}R9.\text{strategyproofness}(1) \) \( \text{R9.\text{support \ lottery-conditions}}[\text{OF R9.wf}] \) \( \text{R9.\text{support}} \) by auto

lemma \( R23 \) [simp]: \( \text{pmf} \ (\text{sds R23}) \ b = 0 \) \( \text{pmf} \ (\text{sds R23}) \ c = 0 \)

pmf \ (\text{sds R23}) \ d = 1 - \ pmf \ (\text{sds R23}) \ a

using \( R23\text{-}R19.\text{strategyproofness}(1) \) \( \text{R23.\text{support \ lottery-conditions}}[\text{OF R23.wf}] \) \( \text{R23.\text{support}} \)

by (auto simp del: pmf-nonneg)

lemma \( R35 \) [simp]: \( \text{pmf} \ (\text{sds R35}) \ a = \text{pmf} \ (\text{sds R21}) \ a \) \( \text{pmf} \ (\text{sds R35}) \ b = 0 \)

pmf \ (\text{sds R35}) \ c = 0 \ pmf \ (\text{sds R35}) \ d = 1 - \ pmf \ (\text{sds R35}) \ a

proof –

from \( R35\text{-}R21.\text{strategyproofness}(1) \) \( \text{R35.\support} \)

have \( \text{pmf} \ (\text{sds R21}) \ a \leq \text{pmf} \ (\text{sds R35}) \ a + \ pmf \ (\text{sds R35}) \ c \) by auto

with \( R21\text{-}R35.\text{strategyproofness}(1) \) \( \text{R35.\support \ lottery-conditions}[\text{OF R35.wf}] \)

show \( \text{pmf} \ (\text{sds R35}) \ a = \text{pmf} \ (\text{sds R21}) \ a \) \( \text{pmf} \ (\text{sds R35}) \ b = 0 \)

pmf \ (\text{sds R35}) \ c = 0 \ pmf \ (\text{sds R35}) \ d = 1 - \ pmf \ (\text{sds R21}) \ a \) by simp-all

14
proof


lemma R18 [simp]: pmf (sds R18) a = pmf (sds R14) a \ \ \ pmf (sds R18) b = 0
pmf (sds R18) d = 0 \ \ \ pmf (sds R18) c = 1 - pmf (sds R14) a

proof –
from R23-R12.strategyproofness(1)
  have R21-R23: pmf (sds R21) a \leq pmf (sds R23) a by simp

from R23-R18.strategyproofness(1)
  have pmf (sds R18) d \leq pmf (sds R21) a - pmf (sds R23) a by simp
also from R21-R23 have \ldots \leq 0 by simp
finally show pmf (sds R18) d = 0 by simp
with lottery-conditions[OF R18.wf] R18.support
  show pmf (sds R18) a = pmf (sds R14) a
    pmf (sds R18) c = 1 - pmf (sds R14) a by auto
qed (insert R18.support, simp-all)

lemma R4 [simp]: pmf (sds R4) a = pmf (sds R21) a \ \ \ pmf (sds R4) b = 0
pmf (sds R4) c = 1 - pmf (sds R4) a \ \ \ pmf (sds R4) d = 0

proof –
from R30-R21.strategyproofness(1) R30.support lottery-conditions[OF R30.wf]
  have pmf (sds R4) c + pmf (sds R21) a \leq pmf (sds R4) c + pmf (sds R30) a by auto
also {
  have pmf (sds R30) a \leq pmf (sds R47) a
    using R47-R30.strategyproofness(1) R30.support R47.support
    lottery-conditions[OF R47.wf] lottery-conditions[OF R47.wf] by auto
  moreover from R4-R47.strategyproofness(1) R4.support R47.support
    lottery-conditions[OF R4.wf] lottery-conditions[OF R47.wf]
    have pmf (sds R4) c \leq pmf (sds R47) c by simp
  ultimately have pmf (sds R4) c + pmf (sds R30) a \leq 1 - pmf (sds R47) d
    using lottery-conditions[OF R47.wf] R47.support by simp
}
finally have pmf (sds R4) c + pmf (sds R14) a \leq 1
using lottery-conditions[OF R47.wf] by (auto simp del: pmf-nonneg)
with R4-R18.strategyproofness(1) lottery-conditions[OF R4.wf] R4.support
  show pmf (sds R4) a = pmf (sds R21) a \ \ \ pmf (sds R4) b = 0
    pmf (sds R4) c = 1 - pmf (sds R4) a \ \ \ pmf (sds R4) d = 0 by auto
qed

lemma R8-d [simp]: pmf (sds R8) d = 1 - pmf (sds R8) a
and R8-c [simp]: pmf (sds R8) c = 0
and R26-a [simp]: pmf (sds R26) a = 1 - pmf (sds R8) a

proof –
from R8-R26.strategyproofness(2) R8.support lottery-conditions[OF R8.wf]
  have pmf (sds R26) a \leq pmf (sds R8) d by auto
with R26-R8.strategyproofness(2) R8.support lottery-conditions[OF R8.wf]
  have pmf (sds R26) a = pmf (sds R8) d by auto
with R8-R26.strategyproofness(2) R8.support lottery-conditions[OF R8.wf]
show \( \text{pmf} \ (\text{sds} \ R8) \ c = 0 \ \text{pmf} \ (\text{sds} \ R8) \ d = 1 - \text{pmf} \ (\text{sds} \ R8) \ a \)
\( \text{pmf} \ (\text{sds} \ R26) \ a = 1 - \text{pmf} \ (\text{sds} \ R8) \ a \) by (auto simp del: pmf-nonneg)

qed

lemma \( R21-R47 \): \( \text{pmf} \ (\text{sds} \ R21) \ d \leq \text{pmf} \ (\text{sds} \ R47) \ c \)
using \( R4-R47.\text{strategyproofness}(1) \ R4.\text{support} \ R47.\text{support} \)
lottery-conditions[\( \text{OF} \ R4.\text{wf} \)] lottery-conditions[\( \text{OF} \ R47.\text{wf} \)]
by auto

lemma \( R30 \) [simp]: \( \text{pmf} \ (\text{sds} \ R30) \ a = \text{pmf} \ (\text{sds} \ R47) \ a \) \( \text{pmf} \ (\text{sds} \ R30) \ b = 0 \)
\( \text{pmf} \ (\text{sds} \ R30) \ c = 0 \) \( \text{pmf} \ (\text{sds} \ R30) \ d = 1 - \text{pmf} \ (\text{sds} \ R47) \ a \)
proof –
\( \text{have} \ A: \ \text{pmf} \ (\text{sds} \ R30) \ a \leq \text{pmf} \ (\text{sds} \ R47) \ a \)
using \( R47-R30.\text{strategyproofness}(1) \ R30.\text{support} \ R47.\text{support} \)
lottery-conditions[\( \text{OF} \ R4.\text{wf} \)] lottery-conditions[\( \text{OF} \ R47.\text{wf} \)] by auto
with \( R21-R47 \ R30-R21.\text{strategyproofness}(1) \)
lottery-conditions[\( \text{OF} \ R30.\text{wf} \)] lottery-conditions[\( \text{OF} \ R47.\text{wf} \)]
show \( \text{pmf} \ (\text{sds} \ R30) \ a = \text{pmf} \ (\text{sds} \ R47) \ a \) \( \text{pmf} \ (\text{sds} \ R30) \ b = 0 \)
\( \text{pmf} \ (\text{sds} \ R30) \ c = 0 \) \( \text{pmf} \ (\text{sds} \ R30) \ d = 1 - \text{pmf} \ (\text{sds} \ R47) \ a \)
by (auto simp: \( \text{R30.\support} \ R47.\support \ \text{simp del: pmf-nonneg} \))

qed

lemma \( R31-c.ge-one-half \): \( \text{pmf} \ (\text{sds} \ R31) \ c \geq 1 / 2 \)
proof –
\( \text{from} \ \text{R25.\support} \ \text{have} \ \text{pmf} \ (\text{sds} \ R25) \ a \geq 1 / 2 \)
proof
\( \text{assume} \ \text{pmf} \ (\text{sds} \ R25) \ c = 0 \)
with \( R25-R36.\text{strategyproofness}(1) \ R36.\text{support} \)
\text{lottery-conditions}[\( \text{OF} \ R36.\text{wf} \)]
\( \text{show} \ \text{pmf} \ (\text{sds} \ R25) \ a \geq 1 / 2 \) by (auto simp del: pmf-nonneg)
next
\( \text{assume} \ \text{[simp]}: \ \text{pmf} \ (\text{sds} \ R25) \ b \ = \ 0 \)
\( \text{from} \ R36-R25.\text{strategyproofness}(1) \ \text{lottery-conditions}[\( \text{OF} \ R25.\text{wf} \)] \)
\( \text{have} \ \text{pmf} \ (\text{sds} \ R25) \ c + \text{pmf} \ (\text{sds} \ R25) \ a \leq \text{pmf} \ (\text{sds} \ R36) \ c + 1 / 2 \) by auto
with \( R25-R36.\text{strategyproofness}(1) \) show \( \text{pmf} \ (\text{sds} \ R25) \ a \geq 1 / 2 \) by auto

qed

hence \( \text{pmf} \ (\text{sds} \ R26) \ a \geq 1 / 2 \)
using \( R25-R26.\text{strategyproofness}(1) \ \text{lottery-conditions}[\( \text{OF} \ R25.\text{wf} \)] \ by \ (auto simp del: pmf-nonneg) \)
with \( \text{lottery-conditions}[\( \text{OF} \ R47.\text{wf} \)] \)
\( \text{have} \ 1 / 2 \leq \text{pmf} \ (\text{sds} \ R26) \ a + \text{pmf} \ (\text{sds} \ R47) \ d \) by (simp del: pmf-nonneg)
also have \( \ldots = 1 - \text{pmf} \ (\text{sds} \ R8) \ a + \text{pmf} \ (\text{sds} \ R47) \ d \) by simp
also from \( R4-R8.\text{strategyproofness}(1) \)
\( \text{have} \ 1 - \text{pmf} \ (\text{sds} \ R8) \ a \leq \text{pmf} \ (\text{sds} \ R21) \ d \) by auto
also note \( R21-R47 \)
also from \( R30-R41.\text{strategyproofness}(1) \ R41.\text{support} \)
\text{lottery-conditions}[\( \text{OF} \ R41.\text{wf} \)] \text{lottery-conditions}[\( \text{OF} \ R47.\text{wf} \)]
\( \text{have} \ \text{pmf} \ (\text{sds} \ R47) \ c + \text{pmf} \ (\text{sds} \ R47) \ d \leq \text{pmf} \ (\text{sds} \ R41) \ d \) by (auto simp del: pmf-nonneg)
also from \textit{R41-R31.strategyproofness}(1) \textit{R41.support lottery-conditions}[OF \textit{R31.wf}]

\textit{lottery-conditions}[OF \textit{R41.wf}]

\textbf{have} pmf \((sds \textit{R41}) \textit{d} \leq pmf \((sds \textit{R31}) \textit{c}\) \textbf{by auto}

\textbf{finally show} pmf \((sds \textit{R31}) \textit{c} \geq 1/2\) \textbf{by simp}

\textit{qed}

\textbf{lemma} \textit{R31}: pmf \((sds \textit{R31}) \textit{a} = 0 \) pmf \((sds \textit{R31}) \textit{c} = 1/2 \) pmf \((sds \textit{R31}) \textit{b} + pmf \((sds \textit{R31}) \textit{d} = 1/2 \)

\textbf{proof} –

\textbf{from} \textit{R2-R38.strategyproofness}(1) \textit{lottery-conditions}[OF \textit{R38.wf}]

\textbf{have} \textit{A}: pmf \((sds \textit{R38}) \textit{b} + pmf \((sds \textit{R38}) \textit{d} \geq 1/2\) \textbf{by auto}

\textbf{with} \textit{R31-c-ge-one-half} \textit{R31-R38.strategyproofness}(1)

\textit{lottery-conditions}[OF \textit{R31.wf}] \textit{lottery-conditions}[OF \textit{R38.wf}]

\textbf{have} pmf \((sds \textit{R38}) \textit{b} + pmf \((sds \textit{R38}) \textit{d} = pmf \((sds \textit{R31}) \textit{d} + pmf \((sds \textit{R31}) \textit{b} \textbf{by auto}

\textbf{with} \textit{R31-c-ge-one-half} \textit{A} \textit{lottery-conditions}[OF \textit{R31.wf}] \textit{lottery-conditions}[OF \textit{R38.wf}]

\textbf{show} pmf \((sds \textit{R31}) \textit{a} = 0\) pmf \((sds \textit{R31}) \textit{c} = 1/2 \) pmf \((sds \textit{R31}) \textit{b} + pmf \((sds \textit{R31}) \textit{d} = 1/2 \)

\textbf{by} \textit{linarith+}

\textit{qed}

\textbf{lemma} \textit{absurd}: \textit{False}

\textbf{using} \textit{R31 R45-R31.strategyproofness}(2) \textbf{by simp}

\textbf{end}

1.4 Lifting to more than 4 agents and alternatives

\textbf{lemma} \textit{finite-list'}:

\textbf{assumes} \textit{finite \textit{A}}
\textbf{obtains} \textit{xs where} \textit{A} = \textit{set xs distinct xs length xs} = \textit{card A}

\textbf{proof} –

\textbf{from} \textit{assms obtain} \textit{xs where} \textit{set xs} = \textit{A} \textbf{using} \textit{finite-list} \textbf{by blast}

\textbf{thus} \textit{thesis} \textbf{using} \textit{distinct-card[of remdups xs]}

\textbf{by} \(\textit{(intro that[of remdups xs]) simp-all}

\textit{qed}

\textbf{lemma} \textit{finite-list-subset}:

\textbf{assumes} \textit{finite \textit{A} \textit{card A} \geq \textit{n}}
\textbf{obtains} \textit{xs where} \textit{set xs} \(\subseteq \textit{A} \textit{distinct xs length xs} = \textit{n}

\textbf{proof} –

\textbf{obtain} \textit{xs where} \textit{A} = \textit{set xs distinct xs length xs} = \textit{card A}
using finite-list[OF assms(1)] by blast
with assms show ?thesis
  by (intro that[of take n xs]) (simp-all add: set-take-subset)
qed

lemma card-ge-4E:
  assumes finite A card A ≥ 4
  obtains a b c d where distinct [a,b,c,d] {a,b,c,d} ⊆ A
proof –
  from assms obtain xs where xs: set xs ⊆ A distinct xs length xs = 4
    by (rule finite-list-subset)
  then obtain a b c d where xs = [a, b, c, d]
    by (auto simp: eval-nat-numeral length-Suc-conv)
  with xs show ?thesis by (intro that[of a b c d]) simp-all
qed

context sds-impossibility
begin

lemma absurd: False
proof –
  from card-ge-4E[OF finite-agents agents-ge-4]
  from card-ge-4E[OF finite-alts alts-ge-4]
  obtain a b c d where alts: distinct [a, b, c, d] {a, b, c, d} ⊆ alts .
  define agents' alts' where agents' = {A1,A2,A3,A4} and alts' = {a,b,c,d}
  from agents alts
    interpret sds-lowering-anonymous-neutral-sdeff-stratproof agents alts sds agents'
    alts'
      unfolding agents'-def alts'-def by unfold-locales simp-all
  from agents alts
    interpret sds-impossibility-4-4 agents' alts' lowered A1 A2 A3 A4 a b c d
      by unfold-locales (simp-all add: agents'-def alts'-def)
  from absurd show False .
qed

end

end

References