https://youtu.be/JrOpdjsq4uo

Hashbasierte Datenstrukturen. 2. Teil: Hash-Bäume[a]

Name: ..... , Vorname: ..... , Klasse: .....

Name Partner: ..... , Klasse: .....

Individueller Parameter k: ..... Datei an Partner: .....

In den nachfolgenden Übungen wird eine "SHA-256"-basierte Hashfunktion verwendet, die im Folgenden als "Stumpfhash" bezeichnet wird. Vom Hash des SHA-256 mit 64 Hex-Zahlen werden nur die ersten fünf Hex-Zahlen genommen und die restlichen 59 werden weggelassen. Z.B. für das kleingeschriebene Wort "world" gilt

SHA-256(world) = 486ea46224d1bb4fb680f34f7c9ad96a8f24ec88be73ea8e5a6c65260e9cb8a7

und

Stumpfhash(world) SH-20(world) = 486ea

Wir betrachten hier nur binäre Hash-Bäume.

1. Übung: Einen Hash-Baum erstellen

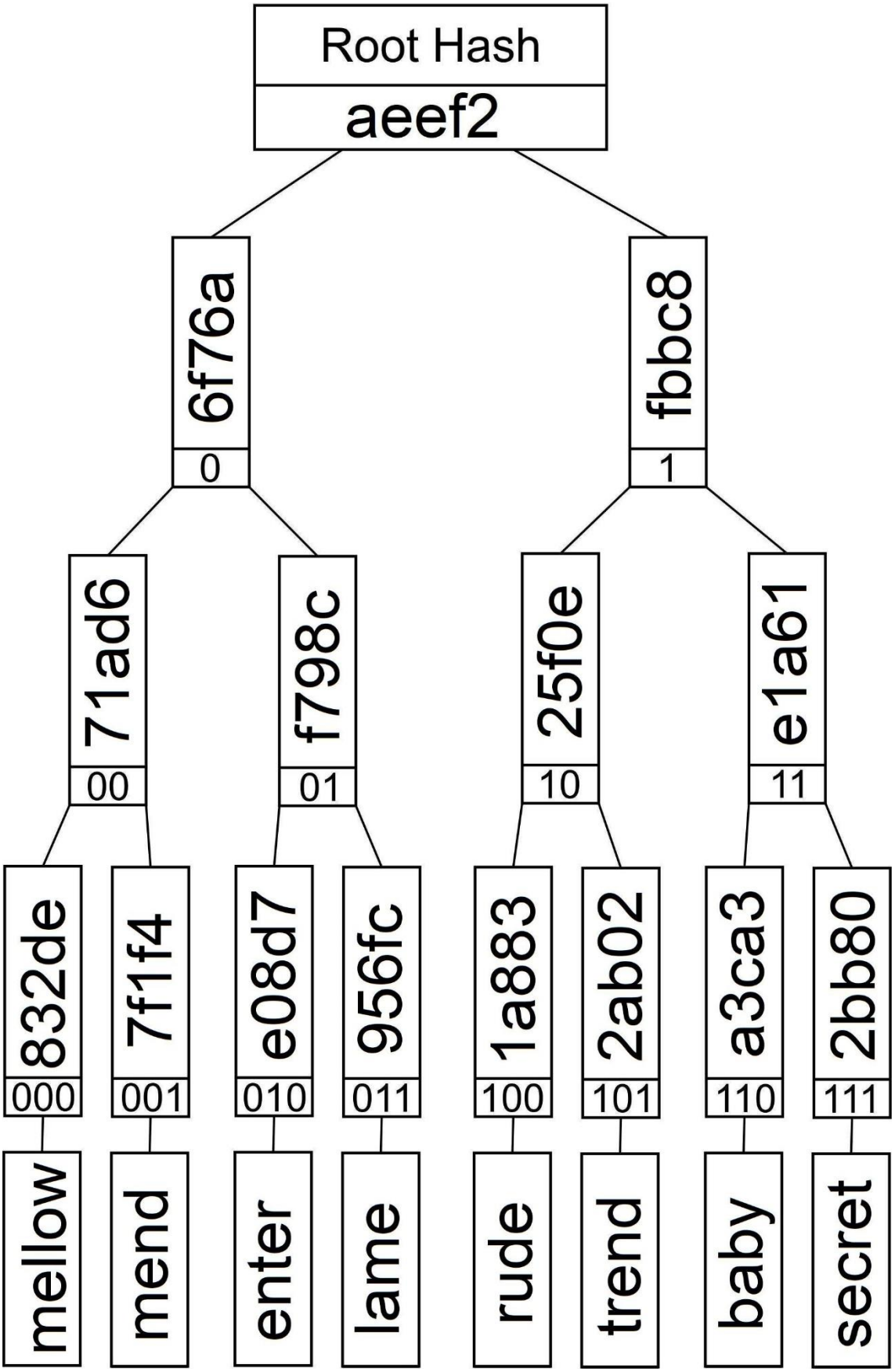
Es seien d000 – d111 Zufallswörter aus der Tabelle von Zufallswörtern im Anhang wie folgt: d000 = Zufallswort(k), d001 = Zufallswort(k + 1), d010 = Zufallswort(k + 2), d011 = Zufallswort(k + 3), d100 = Zufallswort(k + 4), d101 = Zufallswort(k + 5), d110 = Zufallswort(k + 6) und d111 = Zufallswort(k + 7). Dabei ist k der oben handschriftlich notierte individuelle Parameter. Z.B. für k = 18 → d000 = familiar, d001 = elegant, ……. und d111 = imminent.

Siehe dazu untenstehendes Beispiel:

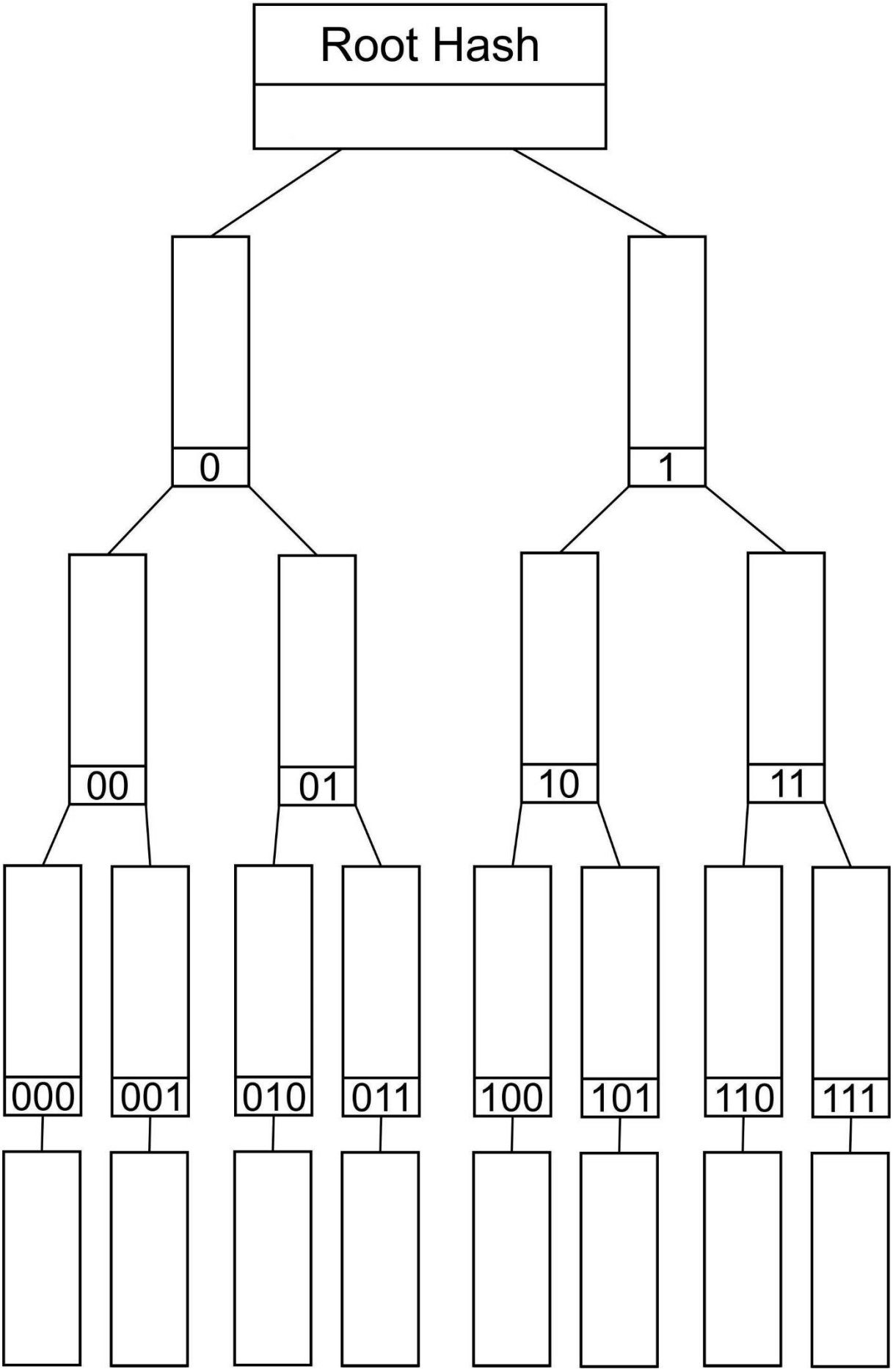
[a] Unterlagen auf https://www.mathepauker.com/Musterex/Benedict/Projektarbeiten/Hash-baeume.pdf

©2020 mathepunk

Beispiel:



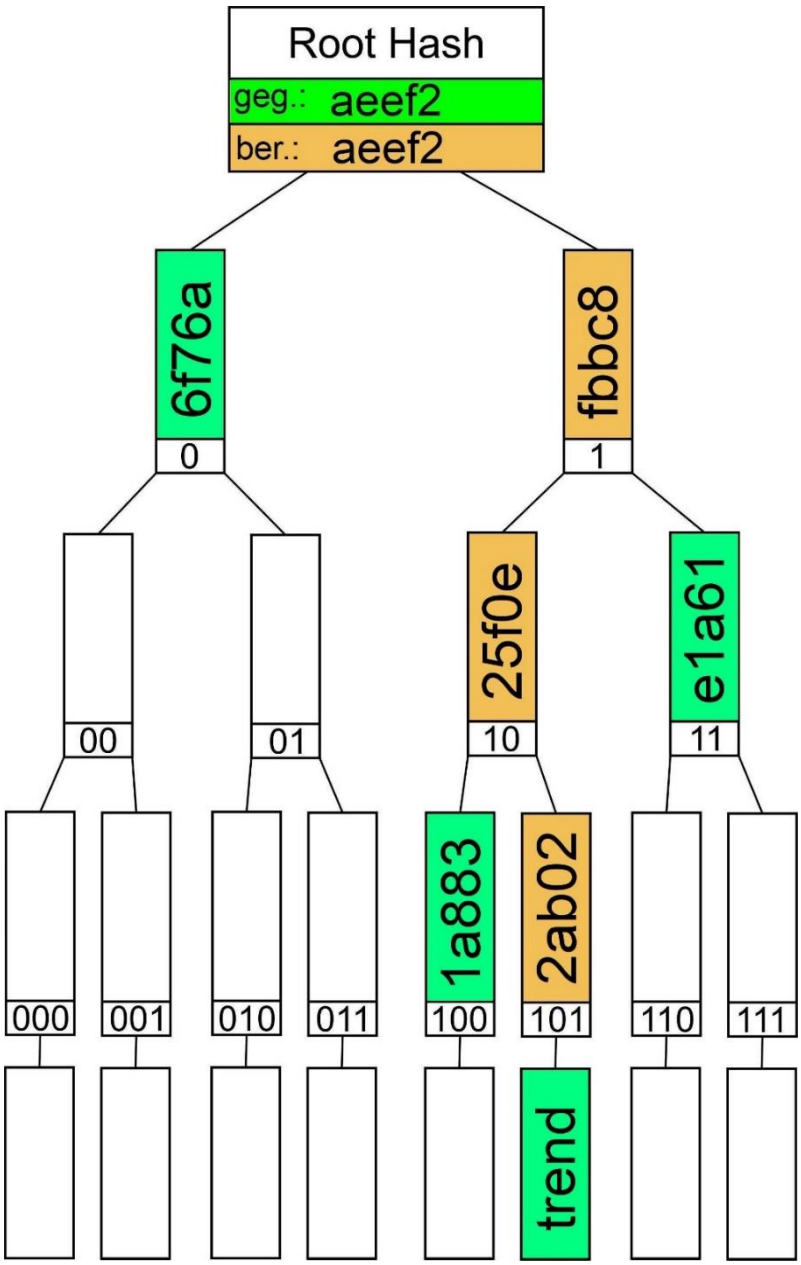
©2020 mathepunk



©2020 mathepunk

2. Übung: "Minimaldaten" für Inklusionsbeweis an Partner übermitteln

Überweise deinem Partner das Zufallswort im Hash-Baum (aus der 1.Übung), das zu Beginn dieses Dokument unter "Datei an Partner" angegeben ist. Ausserdem sollen genau die Hashwerte im Hash-Baum, die für einen Inklusionsbeweis[b] erforderlich sind, mitgeliefert werden. Wenn also z.B. "Datei an Partner: h110", dann soll beim Hash-Baum im obigen Beispiel das Zufallswort "baby" angegeben werden. Neben diesem "richtigen" Zufallswort sollen noch zwei weitere Zufallswörter geliefert werden, ohne Kennzeichnung des "richtigen" Zufallsworts.



In diesem Beispiel soll für die "Datei" d101 des Hash-Baums der Inklusionsbeweis erbracht werden. Dazu werden noch die Hashwerte h100, h11, h0 und der Root

[b] Beweis, dass ein "Blatt" (Datei) zu einem Hash-Baum gehört

©2020 mathepunk

Hash benötigt. Dabei muss auch die "Lage" im Hash-Baum angegeben werden. Mein Partner erhält also die Info

"Dateien": h101 $\in$ {trend, ……} (3 Angaben, zwei "fake", eine richtig)

Hashwerte: h100 = 1a883, h11 = e1a61, h0 = 6f76a und Root Hash = aeef2

Die letzte Angabe ist der Root Hash. Es müssen, wie erwähnt, drei "Dateien" (Zufallswörter) angegeben werden, wovon nur eine die "Richtige" ist, d.h. nur für eine von den dreien kann der Inklusionsbeweis erbracht werden. Es sei SH-20 der zuvor beschriebene "Stumpfhash". Für obiges Beispiel würde dann der Inklusionsbeweis (durch meinen Partner) wie folgt geführt:

SH-20(d101) = h101 = 2ab02

SH-20(h100&h101) = SH-20(1a8832ab02) = h10 = 25f0e

SH-20(h10&h11) = SH-20(25f0ee1a61) = h1 = fbbc8

SH-20(h0&h1) = SH-20(6f76afbbc8) = **Hash Root = aeef2**

Weil der "rekursiv" berechnete Hashwert für die Hash Root mit dem angegebenen Wert aeef2 übereinstimmt ist der Inklusionsbeweis erbracht.

Die Hashwerte in der höchsten Stufe des Hash-Baums werden aus den im Hash-Baum enthaltenen Dateien berechnet. Die Hashwerte auf den oberen Stufen werden aus Hashwerten von Verkettungen zweier Hashwerte berechnet. Bei der Berechnung von Hashwerten ist stets darauf zu achten, dass nicht "unsichtbare" Schriftzeichen durch Betätigen der Leertaste oder der Eingabetaste unbeabsichtigt hinzugefügt werden. Natürlich muss bei der Verkettung von Hashwerten die Reihenfolge beachtet werden. Für h1 $\neq$ h2 gilt SH-20(h1&h2) $\neq$ SH-20(h2&h1), d.h. das Kommutativgesetz gilt nicht.
An den Partner muss die am Anfang dieses Dokuments handschriftlich notierte Datei gegeben werden, zusammen mit den zugehörigen Hashwerten.
In untenstehendem Diagramm sollen die drei "zur Auswahl stehenden" Zufallswörter (Dateien) angegeben werden. Die Position der Datei, d.h. das "Blatt" im Hash-Baum muss gekennzeichnet werden, mit Leuchtstift oder mit einem Pfeil.

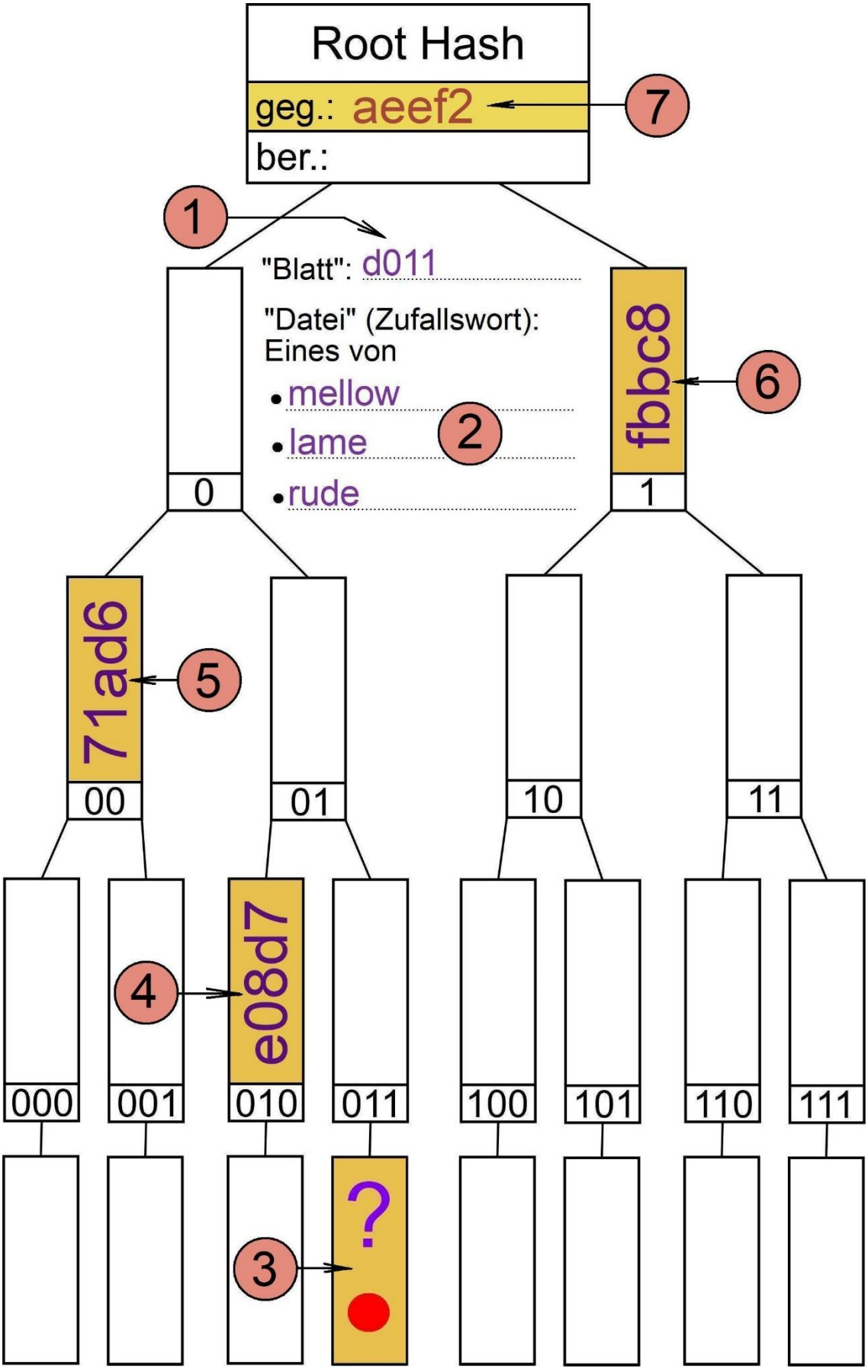
Checkliste:

① "Blatt": Bezeichnung
② Liste mit drei Zufallswörtern
③ "Blatt": Lage im Hash-Baum
④ Hash auf der vierten Stufe
⑤ Hash auf der dritten Stufe
⑥ Hash auf der zweiten Stufe
⑦ Root Hash

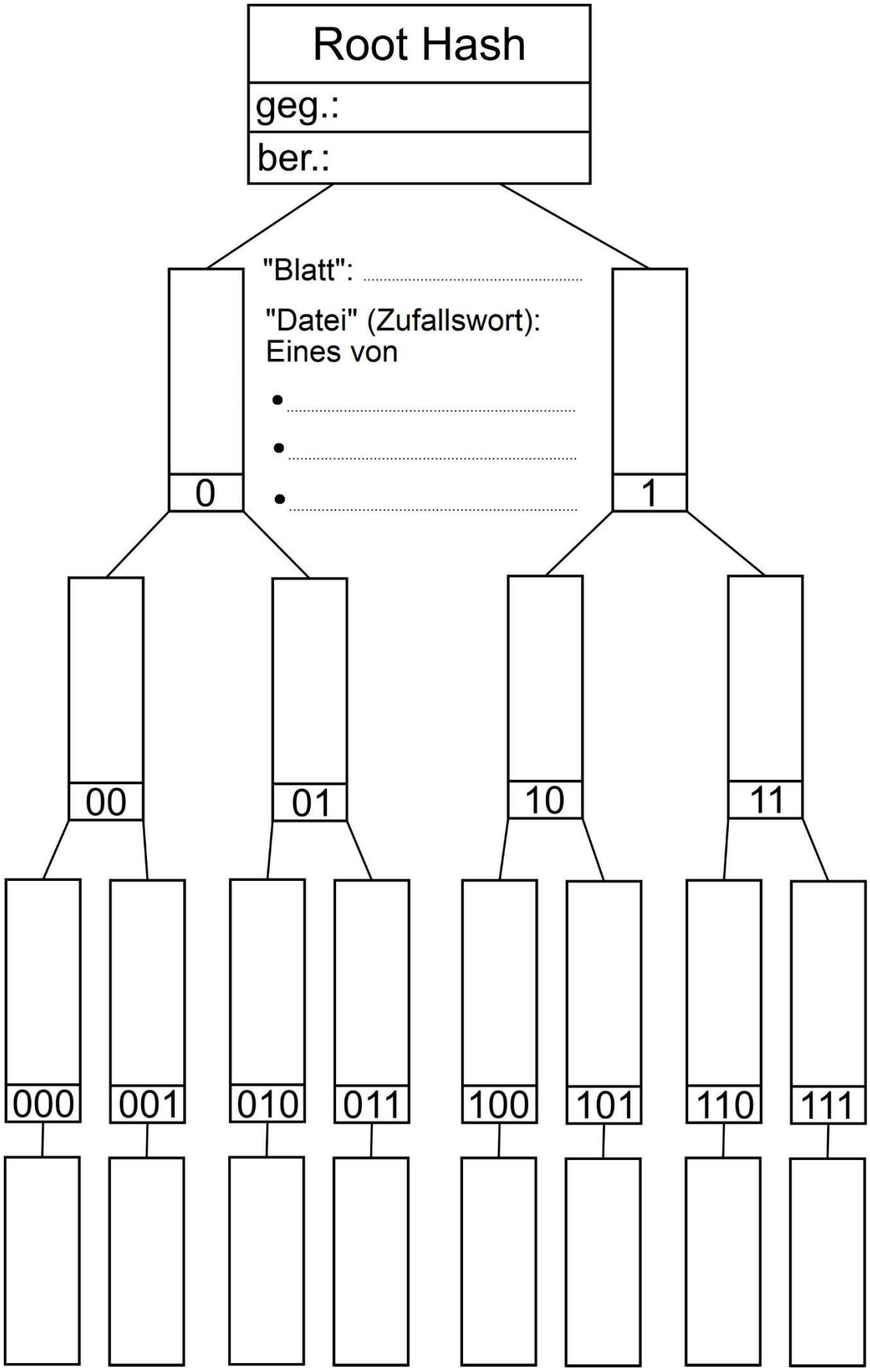
Unten wird für den Hash-Baum aus der 1. Übung (Seite 2), für das "Blatt" d011 gezeigt, welche Info das Diagramm enthalten müsste, das an den Partner abgegeben wird.

©2020 mathepunk

Beispiel für Diagramm, das dem Partner übergeben wird



©2020 mathepunk



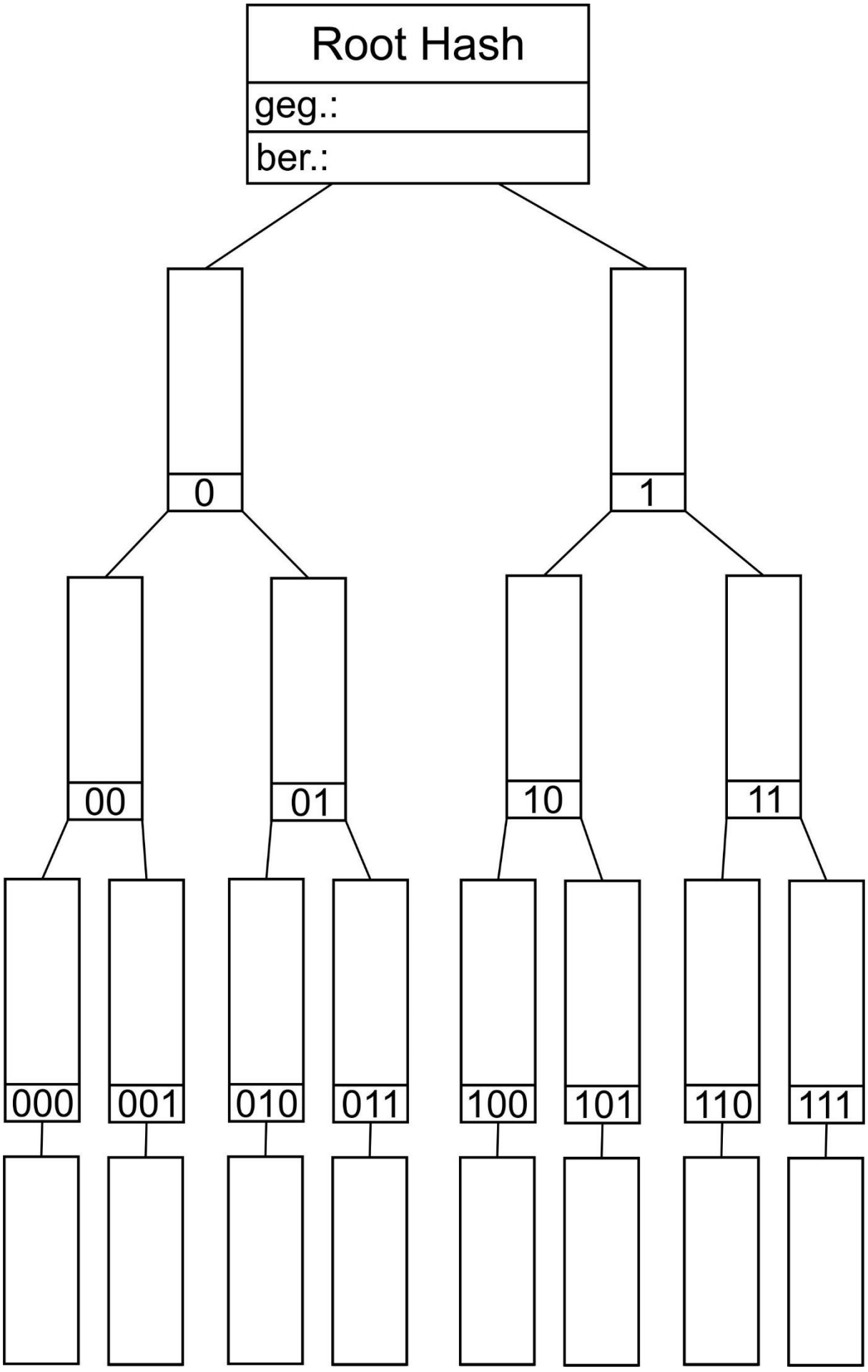
©2020 mathepunk

3. Übung: Mit "Minimaldaten" Inklusionsbeweis erbringen

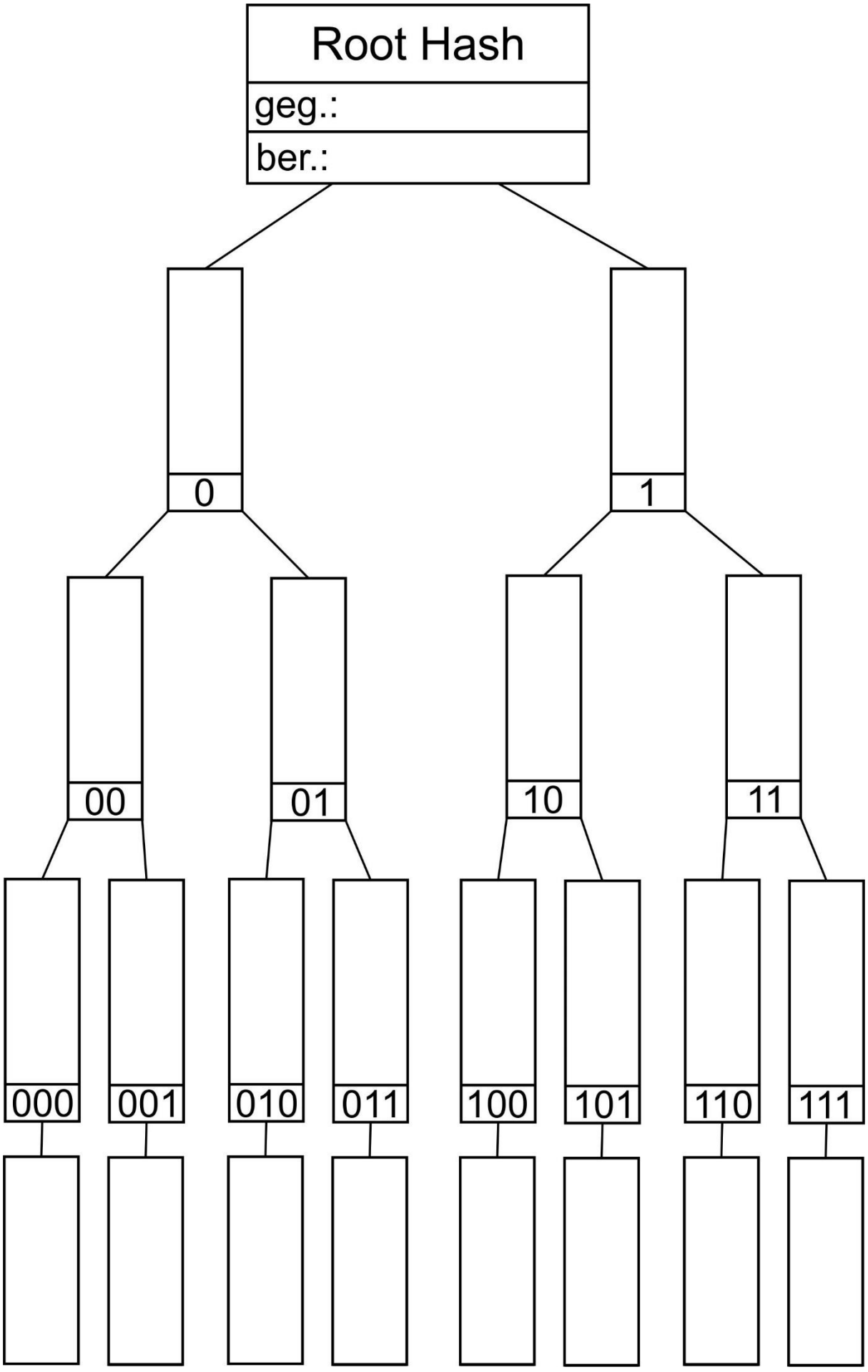
So wie du deinem Partner die minimale Menge an Daten für einen Inklusionsbeweis übermittelt hast, solltest du von deinem Partner wiederum die Angaben erhalten, die für einen Inklusionsbeweis unerlässlich sind. Du erhältst von deinem Partner drei Dateien, von denen nur eine die richtige ist. Die beiden anderen sind "fake". Für jede der drei Dateien muss ein Inklusionsbeweis versucht werden, auch wenn sich der "Erfolg" schon beim ersten Versuch einstellt.

Markiere mit auf den drei nachfolgenden Diagrammen mit Leuchtstift die gegebene "Datei", die gegebenen Hashwerte und die Hashwerte, die man aus den Angaben berechnen kann. Notiere dann die Angaben in den Diagrammen. Berechne die Hashwerte, die man aus den Angaben berechnen kann und notiere sie ebenfalls in den Diagrammen. Siehe dazu das Beispiel Seite 4.

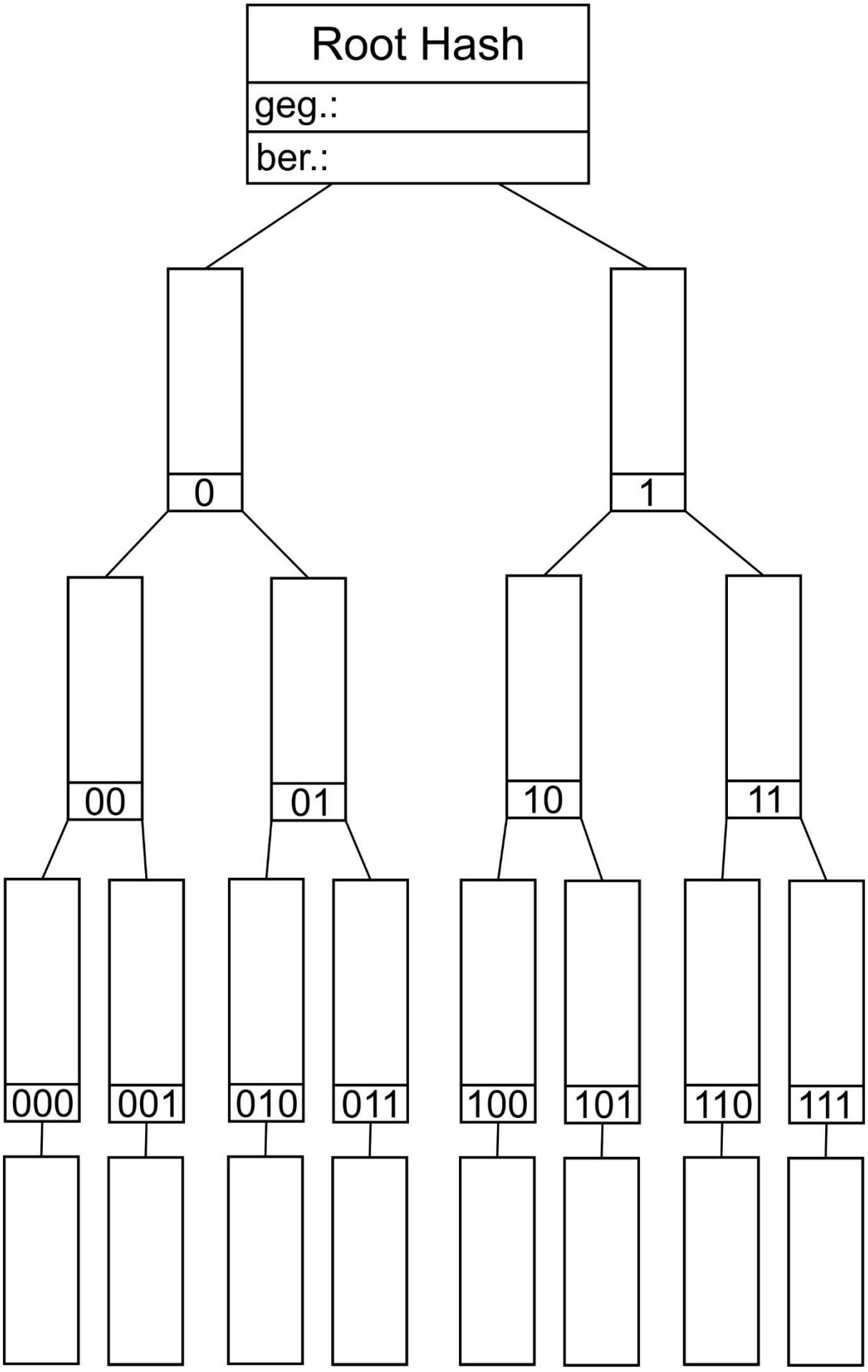
©2020 mathepunk



©2020 mathepunk



©2020 mathepunk



©2020 mathepunk

Anhang

Englische Zufallswörter (k)

1	soap	41	habitual	81	closed	121	seat	161	tooth
2	continue	42	blow	82	jittery	122	post	162	flight
3	industrious	43	front	83	elderly	123	end	163	perpetual
4	pollution	44	dark	84	sincere	124	smelly	164	shop
5	breakable	45	houses	85	cemetery	125	nose	165	hammer
6	breakable	46	party	86	heavenly	126	thick	166	argument
7	pizzas	47	view	87	addition	127	moan	167	impolite
8	heartbreaking	48	amuck	88	baby	128	shock	168	puzzled
9	women	49	overflow	89	wink	129	square	169	pushy
10	substance	50	hypnotic	90	fearless	130	irritate	170	animal
11	remarkable	51	title	91	hole	131	quick	171	rabbits
12	invincible	52	scissors	92	reflect	132	exercise	172	slap
13	evanescent	53	lace	93	amount	133	mend	173	far
14	quack	54	legs	94	quarter	134	zephyr	174	pan
15	outstanding	55	whip	95	rejoice	135	lyrical	175	fireman
16	observant	56	zinc	96	airport	136	enter	176	stretch
17	far-flung	57	punish	97	muddle	137	wide	177	train
18	familiar	58	massive	98	small	138	channel	178	funny
19	elegant	59	thin	99	secret	139	alert	179	quiet
20	adjustment	60	drum	100	roasted	140	sparkling	180	tree
21	troubled	61	treat	101	terrific	141	gainful	181	fallacious
22	mellow	62	pot	102	rude	142	current	182	fence
23	whispering	63	saw	103	lame	143	crime	183	penitent
24	possessive	64	queue	104	able	144	happen	184	last
25	imminent	65	inject	105	quizzical	145	tip	185	well-to-do
26	quarrelsome	66	plucky	106	languid	146	close	186	name
27	eggs	67	start	107	ski	147	exchange	187	rich
28	jagged	68	slip	108	calculator	148	earth	188	unlock
29	committee	69	smart	109	crooked	149	decisive	189	reduce
30	present	70	copy	110	promise	150	grape	190	loving
31	guard	71	mine	111	swim	151	governor	191	frequent
32	uttermost	72	clean	112	dance	152	hanging	192	wrist
33	giraffe	73	tramp	113	eye	153	fluttering	193	hideous
34	belligerent	74	mint	114	guarded	154	glossy	194	vegetable
35	harmonious	75	spill	115	separate	155	bustling	195	twig
36	stupendous	76	hour	116	tedious	156	greasy	196	crook
37	development	77	milk	117	pig	157	volleyball	197	allow
38	damaged	78	practise	118	rat	158	entertain	198	powder
39	office	79	chance	119	scene	159	leather	199	train
40	fancy	80	anxious	120	trade	160	blush	200	drain

©2020 mathepunk