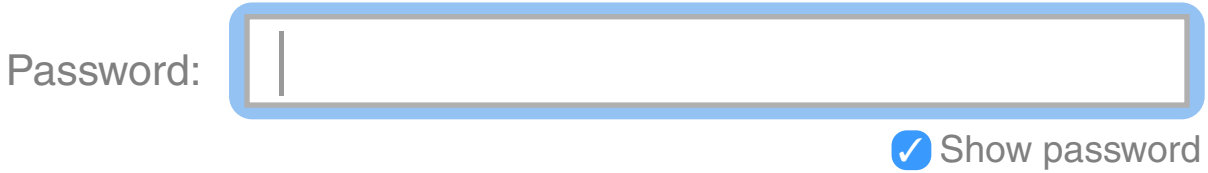
A Large-scale Analysis of the Mnemonic Password Advice

Johannes Kiesel, Benno Stein, Stefan Lucks
Bauhaus-Universität Weimar
www.webis.de

NDSS 2017, February 27th 2017

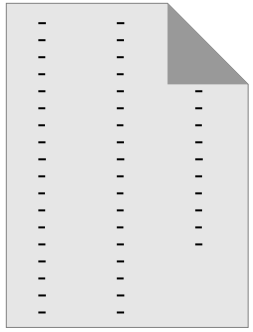
Mnemonic Password Creation

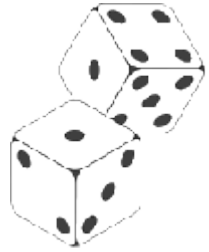


Mnemonic Password Creation

Password: wxW,2bs%)0

☑ Show password



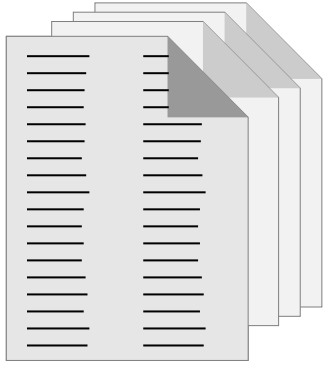


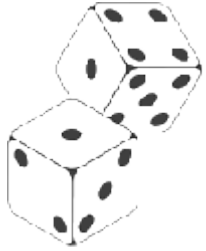
	Random characters (out of 96)
$H_1 \approx 65$ Bit (requires botnet)	10 chars

Mnemonic Password Creation

Password: embalm fuss yogi layup plague

☑ Show password





	Random characters (out of 96)	Random words (out of 7776)
$H_1 \approx 65$ Bit (requires botnet)	10 chars	5 words

Mnemonic Password Creation

Password: tnciagptmip

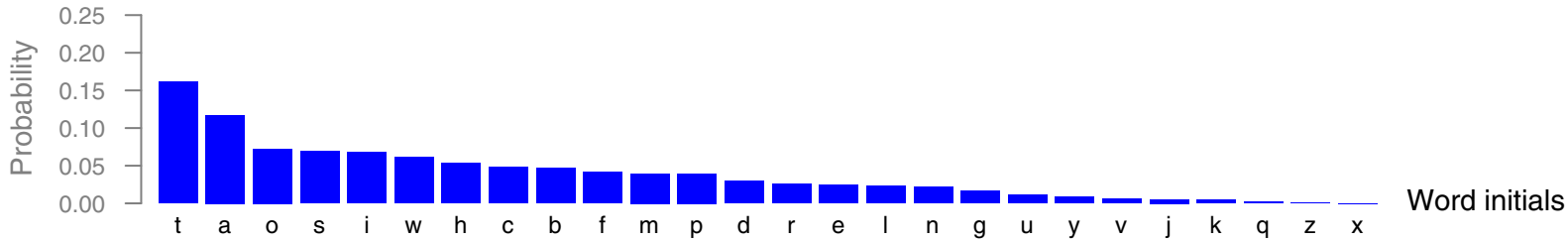
☑ Show password

"The NDSS conference is a great place to meet interesting people!"

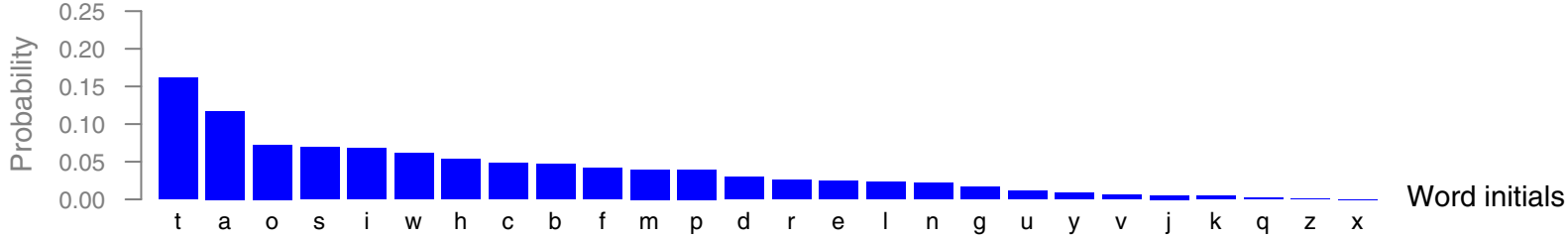
(Password advice given by the German Federal Office for Information Security, Google, etc.)

	Random characters (out of 96)	Random words (out of 7776)	Mnemonic sentence (human mind)
$H_1 \approx 65$ Bit (requires botnet)	10 chars	5 words	?

Frequency and Correlation in Natural Language



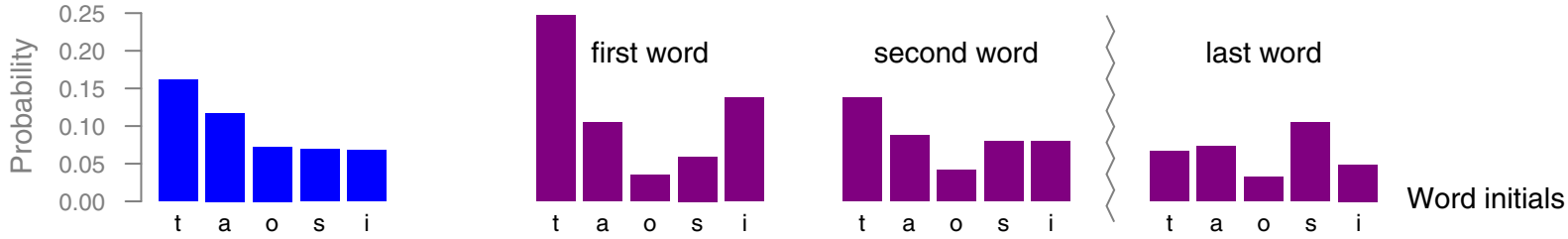
Frequency and Correlation in Natural Language



successor

predecessor	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
a	.1009	.0394	.0547	.0316	.0274	.0455	.0212	.0489	.0596	.0055	.0050	.0347	.0470	.0243	.0517	.0475	.0029	.0306	.0784	.1619	.0110	.0089
b	.1381	.0326	.0461	.0319	.0234	.0357	.0147	.0558	.0722	.0060	.0043	.0198	.0384	.0196	.0734	.0352	.0019	.0278	.0693	.1726	.0154	.0051
c	.1368	.0609	.0409	.0280	.0210	.0464	.0135	.0450	.0779	.0046	.0029	.0172	.0290	.0179	.1177	.0309	.0012	.0230	.0568	.1269	.0138	.0048
d	.1279	.0497	.0401	.0208	.0181	.0443	.0108	.0443	.0821	.0050	.0066	.0170	.0281	.0435	.1044	.0320	.0015	.0193	.0551	.1557	.0112	.0039
e	.1225	.0423	.0446	.0266	.0228	.0475	.0142	.0351	.0897	.0033	.0043	.0180	.0342	.0147	.1178	.0389	.0014	.0223	.0627	.1505	.0100	.0052
f	.1379	.0369	.0424	.0267	.0286	.0352	.0149	.0512	.0669	.0047	.0028	.0198	.0413	.0129	.0771	.0363	.0014	.0229	.0581	.2013	.0096	.0058
g	.1482	.0456	.0443	.0309	.0201	.0402	.0127	.0530	.0718	.0054	.0040	.0181	.0389	.0141	.0932	.0349	.0013	.0241	.0617	.1388	.0195	.0060
h	.1083	.0795	.0518	.0358	.0255	.0456	.0183	.0711	.0506	.0051	.0076	.0302	.0372	.0275	.0524	.0364	.0014	.0286	.0838	.1052	.0092	.0060
i	.1265	.0301	.0459	.0294	.0220	.0315	.0158	.0515	.0725	.0045	.0050	.0189	.0351	.0280	.0538	.0331	.0018	.0234	.0606	.2136	.0090	.0058
j	.1613	.0645	.0581	.0323	.0172	.0452	.0237	.0581	.0473	.0129	.0086	.0258	.0387	.0129	.0559	.0301	.0022	.0280	.0688	.1097	.0065	.0043
k	.1298	.0336	.0336	.0224	.0157	.0313	.0112	.0828	.0761	.0067	.0067	.0157	.0268	.0157	.1230	.0179	.0022	.0179	.0537	.1588	.0112	.0045
l	.1554	.0427	.0398	.0277	.0204	.0437	.0151	.0491	.0738	.0068	.0034	.0228	.0340	.0165	.0942	.0345	.0024	.0219	.0583	.1452	.0165	.0058
m	.1266	.0656	.0463	.0305	.0236	.0420	.0158	.0527	.0647	.0075	.0060	.0262	.0340	.0184	.1010	.0423	.0020	.0256	.0665	.1131	.0124	.0063
n	.1100	.0519	.0519	.0332	.0322	.0436	.0187	.0446	.0545	.0062	.0083	.0327	.0503	.0176	.0949	.0415	.0036	.0322	.0669	.1105	.0104	.0078
o	.1070	.0292	.0502	.0251	.0266	.0318	.0162	.0510	.0439	.0057	.0033	.0215	.0433	.0169	.0576	.0408	.0012	.0222	.0623	.2837	.0086	.0070
p	.1393	.0406	.0486	.0270	.0225	.0474	.0130	.0409	.0871	.0044	.0056	.0169	.0296	.0116	.1337	.0317	.0015	.0216	.0554	.1263	.0139	.0056
q	.1824	.0353	.0471	.0294	.0235	.0412	.0118	.0353	.0706	.0059	.0000	.0176	.0294	.0176	.1294	.0294	.0000	.0235	.0765	.0882	.0118	.0059

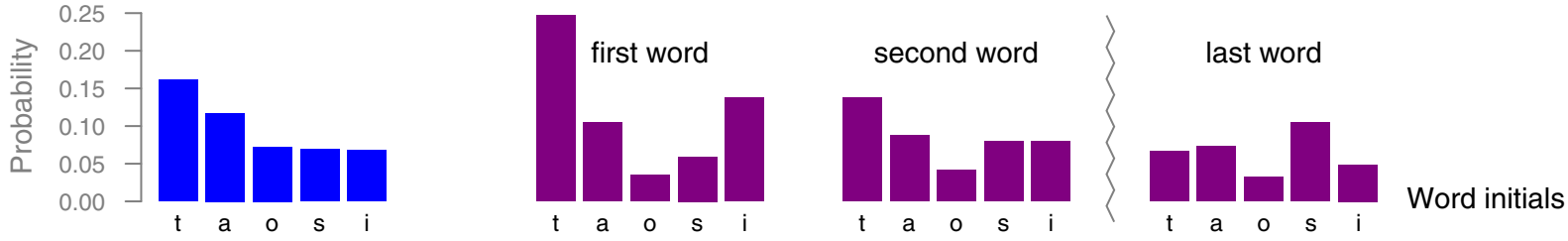
Frequency and Correlation in Natural Language



successor

predecessor	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
a	.1009	.0394	.0547	.0316	.0274	.0455	.0212	.0489	.0596	.0055	.0050	.0347	.0470	.0243	.0517	.0475	.0029	.0306	.0784	.1619	.0110	.0089
b	.1381	.0326	.0461	.0319	.0234	.0357	.0147	.0558	.0722	.0060	.0043	.0198	.0384	.0196	.0734	.0352	.0019	.0278	.0693	.1726	.0154	.0051
c	.1368	.0609	.0409	.0280	.0210	.0464	.0135	.0450	.0779	.0046	.0029	.0172	.0290	.0179	.1177	.0309	.0012	.0230	.0568	.1269	.0138	.0048
d	.1279	.0497	.0401	.0208	.0181	.0443	.0108	.0443	.0821	.0050	.0066	.0170	.0281	.0435	.1044	.0320	.0015	.0193	.0551	.1557	.0112	.0039
e	.1225	.0423	.0446	.0266	.0228	.0475	.0142	.0351	.0897	.0033	.0043	.0180	.0342	.0147	.1178	.0389	.0014	.0223	.0627	.1505	.0100	.0052
f	.1379	.0369	.0424	.0267	.0286	.0352	.0149	.0512	.0669	.0047	.0028	.0198	.0413	.0129	.0771	.0363	.0014	.0229	.0581	.2013	.0096	.0058
g	.1482	.0456	.0443	.0309	.0201	.0402	.0127	.0530	.0718	.0054	.0040	.0181	.0389	.0141	.0932	.0349	.0013	.0241	.0617	.1388	.0195	.0060
h	.1083	.0795	.0518	.0358	.0255	.0456	.0183	.0711	.0506	.0051	.0076	.0302	.0372	.0275	.0524	.0364	.0014	.0286	.0838	.1052	.0092	.0060
i	.1265	.0301	.0459	.0294	.0220	.0315	.0158	.0515	.0725	.0045	.0050	.0189	.0351	.0280	.0538	.0331	.0018	.0234	.0606	.2136	.0090	.0058
j	.1613	.0645	.0581	.0323	.0172	.0452	.0237	.0581	.0473	.0129	.0086	.0258	.0387	.0129	.0559	.0301	.0022	.0280	.0688	.1097	.0065	.0043
k	.1298	.0336	.0336	.0224	.0157	.0313	.0112	.0828	.0761	.0067	.0067	.0157	.0268	.0157	.1230	.0179	.0022	.0179	.0537	.1588	.0112	.0045
l	.1554	.0427	.0398	.0277	.0204	.0437	.0151	.0491	.0738	.0068	.0034	.0228	.0340	.0165	.0942	.0345	.0024	.0219	.0583	.1452	.0165	.0058
m	.1266	.0656	.0463	.0305	.0236	.0420	.0158	.0527	.0647	.0075	.0060	.0262	.0340	.0184	.1010	.0423	.0020	.0256	.0665	.1131	.0124	.0063
n	.1100	.0519	.0519	.0332	.0322	.0436	.0187	.0446	.0545	.0062	.0083	.0327	.0503	.0176	.0949	.0415	.0036	.0322	.0669	.1105	.0104	.0078
o	.1070	.0292	.0502	.0251	.0266	.0318	.0162	.0510	.0439	.0057	.0033	.0215	.0433	.0169	.0576	.0408	.0012	.0222	.0623	.2837	.0086	.0070
p	.1393	.0406	.0486	.0270	.0225	.0474	.0130	.0409	.0871	.0044	.0056	.0169	.0296	.0116	.1337	.0317	.0015	.0216	.0554	.1263	.0139	.0056
q	.1824	.0353	.0471	.0294	.0235	.0412	.0118	.0353	.0706	.0059	.0000	.0176	.0294	.0176	.1294	.0294	.0000	.0235	.0765	.0882	.0118	.0059

Frequency and Correlation in Natural Language



successor

predecessor	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
a	.1009	.0394	.0547	.0316	.0274	.0455	.0212	.0489	.0596	.0055	.0050	.0347	.0470	.0243	.0517	.0475	.0029	.0306	.0784	.1619	.0110	.0089
b	.1381	.0326	.0461	.0319	.0234	.0357	.0147	.0558	.0722	.0060	.0043	.0198	.0384	.0196	.0734	.0352	.0019	.0278	.0693	.1726	.0154	.0051
c	.1368	.0609	.0409	.0280	.0210	.0464	.0135	.0450	.0779	.0046	.0029	.0172	.0290	.0179	.1177	.0309	.0012	.0230	.0568	.1269	.0138	.0048
d	.1279	.0497	.0401	.0208	.0181	.0443	.0108	.0443	.0821	.0050	.0066	.0170	.0281	.0435	.1044	.0320	.0015	.0193	.0551	.1557	.0112	.0039
e	.1225	.0423	.0446	.0266	.0228	.0475	.0142	.0351	.0897	.0033	.0043	.0180	.0342	.0147	.1178	.0389	.0014	.0223	.0627	.1505	.0100	.0052
f	.1379	.0369	.0424	.0267	.0286	.0352	.0149	.0512	.0669	.0047	.0028	.0198	.0413	.0129	.0771	.0363	.0014	.0229	.0581	.2013	.0096	.0058
g	.1482	.0456	.0443	.0309	.0201	.0402	.0127	.0530	.0718	.0054	.0040	.0181	.0389	.0141	.0932	.0349	.0013	.0241	.0617	.1388	.0195	.0060
h	.1083	.0795	.0518	.0358	.0255	.0456	.0183	.0711	.0506	.0051	.0076	.0302	.0372	.0275	.0524	.0364	.0014	.0286	.0838	.1052	.0092	.0060
i	.1265	.0301	.0459	.0294	.0220	.0315	.0158	.0515	.0725	.0045	.0050	.0189	.0351	.0280	.0538	.0331	.0018	.0234	.0606	.2136	.0090	.0058
j	.1613	.0645	.0581	.0323	.0172	.0452	.0237	.0581	.0473	.0129	.0086	.0258	.0387	.0129	.0559	.0301	.0022	.0280	.0688	.1097	.0065	.0043
k	.1298	.0336	.0336	.0224	.0157	.0313	.0112	.0828	.0761	.0067	.0067	.0157	.0268	.0157	.1230	.0179	.0022	.0179	.0537	.1588	.0112	.0045
l	.1554	.0427	.0398	.0277	.0204	.0437	.0151	.0491	.0738	.0068	.0034	.0228	.0340	.0165	.0942	.0345	.0024	.0219	.0583	.1452	.0165	.0058
m	.1266	.0656	.0463	.0305	.0236	.0420	.0158	.0527	.0647	.0075	.0060	.0262	.0340	.0184	.1010	.0423	.0020	.0256	.0665	.1131	.0124	.0063
n	.1100	.0519	.0519	.0332	.0322	.0436	.0187	.0446	.0545	.0062	.0083	.0327	.0503	.0176	.0949	.0415	.0036	.0322	.0669	.1105	.0104	.0078
o	.1070	.0292	.0502	.0251	.0266	.0318	.0162	.0510	.0439	.0057	.0033	.0215	.0433	.0169	.0576	.0408	.0012	.0222	.0623	.2837	.0086	.0070
p	.1393	.0406	.0486	.0270	.0225	.0474	.0130	.0409	.0871	.0044	.0056	.0169	.0296	.0116	.1337	.0317	.0015	.0216	.0554	.1263	.0139	.0056
q	.1824	.0353	.0471	.0294	.0235	.0412	.0118	.0353	.0706	.0059	.0000	.0176	.0294	.0176	.1294	.0294	.0000	.0235	.0765	.0882	.0118	.0059

➜ Position-dependent, higher-order language model learning on Big data.

Challenge: Building a Corpus for Mnemonic Analyses

Q. How many sentences do we need?

A. The more the better: 10^8 sentences for training 7th order model

≈ 5,000	Mnemonics	Study by Yang et al., 2016
≈ 80,000	Sentences	The Bible
≈ 5,000,000	Sentences	Encyclopedia Britannica
730,000,000	Web pages	ClueWeb12, 27.3 TB
3,400,000,000	Sentences	extracted and filtered

Challenge: Building a Corpus for Mnemonic Analyses

Q. How many sentences do we need?

A. The more the better: 10^8 sentences for training 7th order model

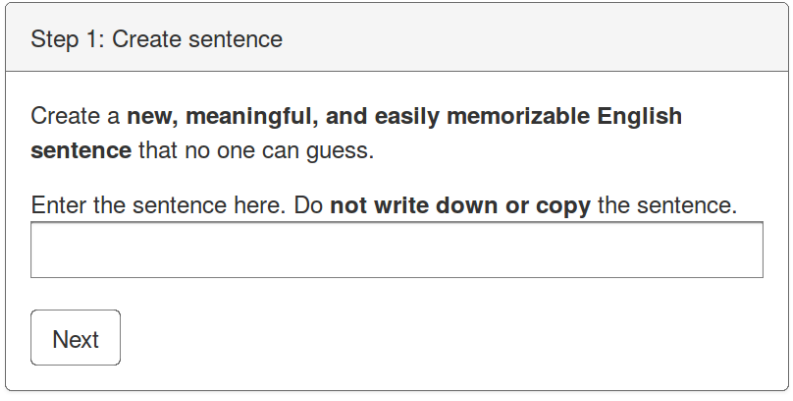
≈ 5,000	Mnemonics	Study by Yang et al., 2016
≈ 80,000	Sentences	The Bible
≈ 5,000,000	Sentences	Encyclopedia Britannica
730,000,000	Web pages	ClueWeb12, 27.3 TB
3,400,000,000	Sentences	extracted and filtered

Q. Are web sentences and password mnemonics of the same language?

A. Compare to mnemonics from a MTurk study

Steps: (1) Mnemonic, (2) password, (3) questions, (4) recall

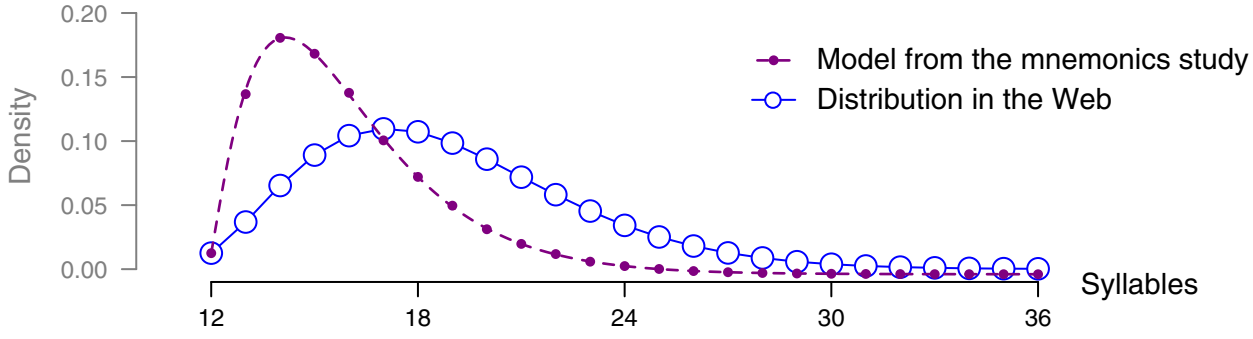
1,117	Participants
1,048	Mnemonics
$0.15	Payment
3 min 38 sec	Average time



Challenge: Building a Corpus for Mnemonic Analyses (contd.)

Q. Are web sentences and password mnemonics of the same sentence complexity?

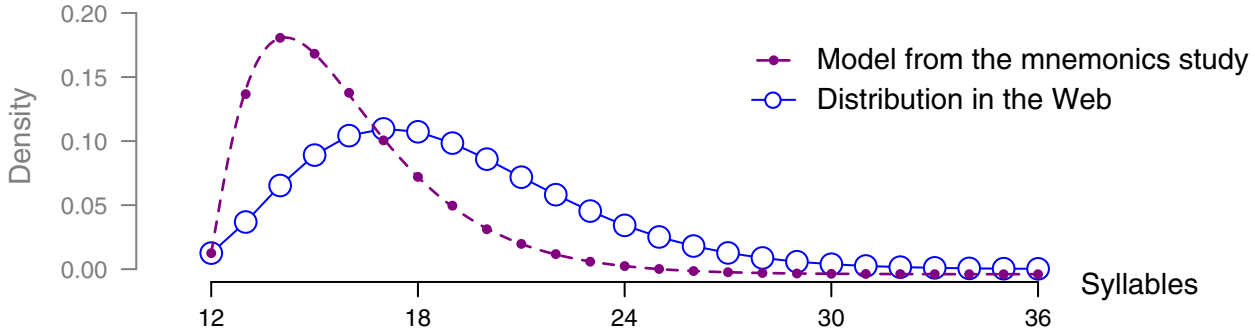
A. Analyze syllable counts as measure of readability



Challenge: Building a Corpus for Mnemonic Analyses (contd.)

Q. Are web sentences and password mnemonics of the same sentence complexity?

A. Analyze syllable counts as measure of readability



Q. Contain web sentences and password mnemonics similar phrases?

A. Analyze predictability (H_1 in Bit) of word initials within and across corpora

Model from	Predicting	Model order				
		0	1	2	3	4
Mnemonics	Mnemonics	4.59	**4.51**	4.54	4.55	4.55
Simple web sentences	Mnemonics	4.94	4.63	4.56	**4.55**	4.62

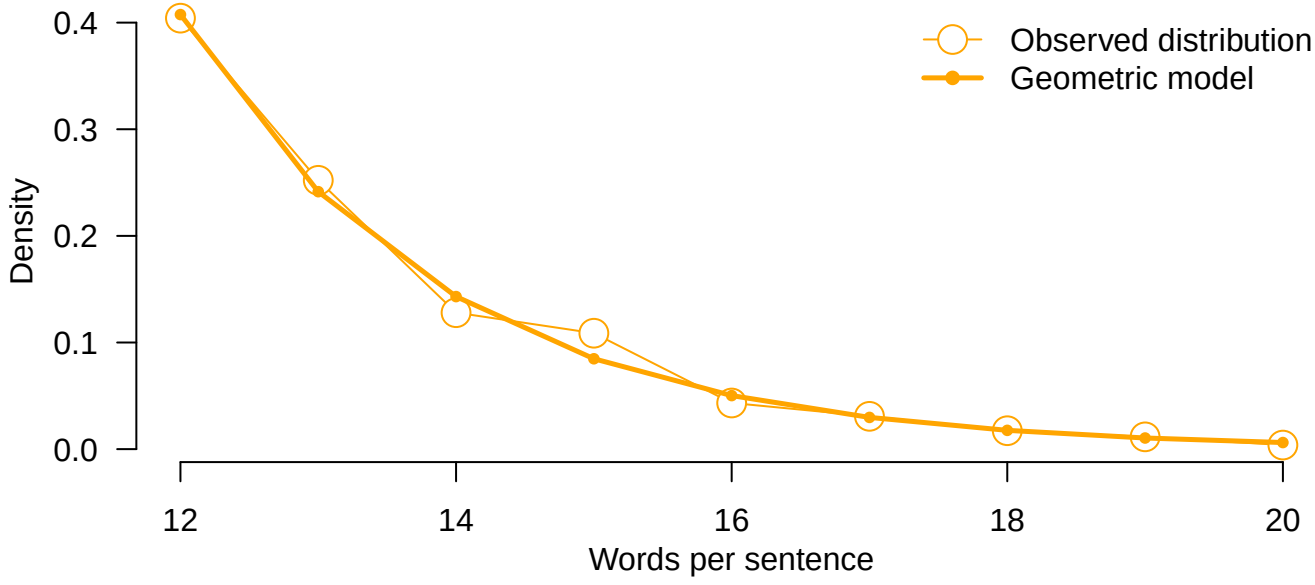
Mnemonic Password Creation: Selected Results

	Random characters (out of 96)	Random words (out of 7776)	Mnemonic sentence (human mind)
$H_1 \approx 65$ Bit (requires botnet)	10 chars	5 words	13+ words

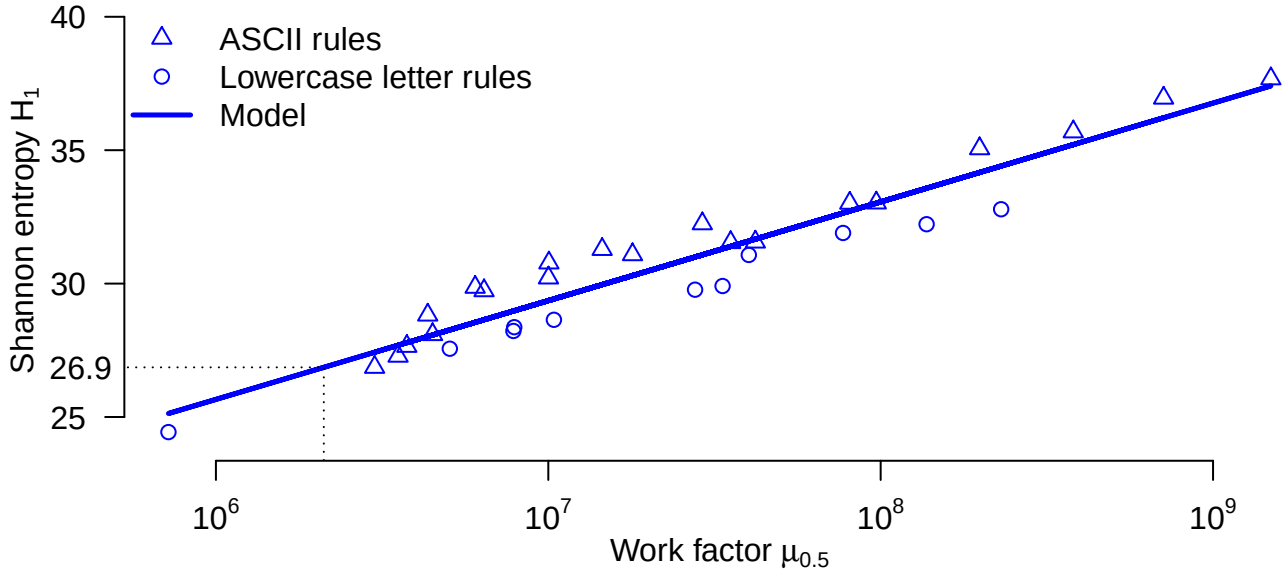
- Lowercase password from sentence with 13 or more words — 54 Bit
- 7-bit visible ASCII (incl. %, !, @, #, etc.) — 8 Bit
  adds on average 2 characters, worth 6.4 Bit alone
- Word replacements (for $\rightarrow$ 4, at $\rightarrow$ @) — 2 Bit
- Different characters (last of each word instead of first) — 0 Bit
- Complex sentences (rich vocabulary) — + 2 Bit

66 Bit

Appendix: Mnemonics Study Sentence Length



Appendix: Correlation Work-factor and Entropy



Appendix: Example Sentences

Mnemonics

- What was the color of your car when you were twenty years old?
- The order of my favorite colors followed by my cousin's pets is the password that I use.
- beautiful mails require a touch of golden heart and brave minds that also pray
- Savings under the floorboards are safer than inside a big bank vault.
- While shopping i usually purchase meaningless items that i wrap up in shinny paper.
- when I don't have money I want it, if I have money I want more.
- Cash is king of the hill and worth every penny and cent.
- The crisp green bill did not leave the frugal boy's pocket until the day he died.
- I told my friend a secret and told her not to tell anyone

Web Sentences

- The ADA recommends that the costs associated with postexposure prophylaxis and exposure sequelae be a benefit of Workers' Compensation insurance coverage.
- Your agents will come away with the knowledge of how service level and quality go hand-in-hand and how that affects the entire contact center.
- The arena act was the product of gate keeping & was only ever important from a commercial standpoint.

Simple Web Sentences

- Please do not ask to return an item after 7 days of when you received the item.
- This guide has a lot of nuggets, and I could only stop when I was finished with it.
- She acted as a student leader during her primary school, high school, college and graduate studies.