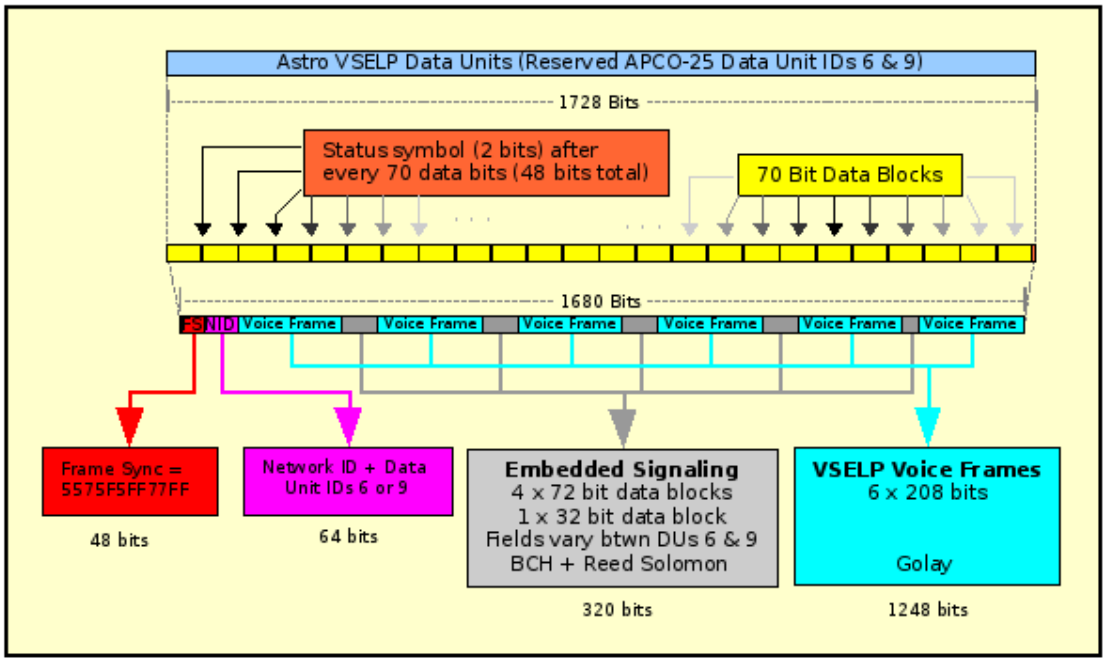
Treading On VSELP Astro Turf
(As implemented by Motorola Using the APCO-25 CAI)

Huntsville Alabama has a Motorola VSELP repeater output at 172.475 MHz in the federal band. We have started harvesting information from this system using an Ettus Research USRP and GNU Radio system. The air interface is identical to the APCO 25 CAI up until voice data units are transmitted. We assume some familiarity with the APCO 25 CAI standards; all the information needed to understand the information presented in this section can be found in the Daniels Electronics LTD P25 training guide.
We note that the traffic on this system is far too structured to be encrypted. In particular, VSELP voice frames encoding 30 ms of silence are readily identifiable and distributed in the expected manner (such as a heavy clustering at the end of transmissions). It is worth noting that these silent frames are deliberately inserted at the end of transmissions - cf U.S. Patent 5220565 which also obligingly lists the 144 VSELP data bits which when error protected turn into 208 bit blocks transmitted over the air.

Without further ado we present a diagram of the air interface used to transmit VSELP Astro data over the APCO-25 CAI; more details may be presented as time and motivation permit.

Transmission of Motorola ASTRO VSELP Data Frames Using APCO-25 CAI

Everything is APCO-25 compliant (header data units, terminator data units, frame sync, network id, et cetera) except LDU1 & LDU2 IMBE Voice Data Units are replaced by VSELP Data Units as shown below:



Running some numbers

```
180 mS  :   Time to transmit one 1728 bit VSELP data unit
 30 mS  :   Milliseconds of speech data covered by one VSELP frame
```

```
2.7 kbps:   Aggregate bit rate, embedded signaling
6.9 kbps:   Aggregate bit rate, VSELP Voice Frames
            (2.1 kbps devoted to error correction)

9.6 kbps:   Total transmission bit rate
```

Some Preliminary Notes - Motorola VSELP Data Frame

Let us number the 208 received bits of a VSELP frame in order as they are received from zero to 207. If we then place these bits into a table sized to match the apparent interleave pattern, and highlight some related bits we end up with something like the following:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167
168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207								

Color key:

Color	Bits	Comments
	17	Block Code (Hamming Distance 7)
	17	Block Code (Hamming Distance 7)

	23	GOLAY (23,12,7)
	23	GOLAY (23,12,7)
	23	GOLAY (23,12,7)
	8	Speculative grouping
	3	Always Zero

Comments:

We note that even indices naturally have better error protection as a result of 4-Level FSK modulation. And indeed, those bits that have error protection coding tend to fall on even indices. There is obviously still a long way to go on the analysis.

The information in this section is subject to change. The identification and location of the three Golay (23,13) data blocks are almost certainly correct. The 17 bit blocks shown in green and violet are definitely related - treated as 17 bit data words they exhibit a 7 bit minimum Hamming distance sufficient to correct any three bit errors; it might however be premature to chalk this up to something like a (17,8,7) or similar block code. More work may turn up further correlated bit groups such as that speculative 8 bit grouping.

While there is some possibility that this work by itself could lead to an decoder that produces intelligible ASTRO VSELP speech it is far more likely that VSELP test frames will have to be constructed and fed into surplus radio equipment in order to back out bit functions, voice code tables, et cetera. This is the impetus for for characterizing the error correcting coding. Getting surplus radio equipment is not a problem since this mode is technically obsolete and most everyone is migrating to fully APCO-25 compliant systems (although *certain* legacy governmental ASTRO VSELP systems will likely remain in use for years to come).

Although not necessary for further progress, much more will be learned if this information can be successfully correlated with U.S. Patent 5220565.
